مدينة الملك عبد العزيز للعلوم والتقنية
المنظمة العربية للترجمة

لورنس م. أوليفا

أمن تقنية المعلومات

نصائح من خبراء



ترجمة
د. محمد مراياتي

سلسلة كتب التقنيات الاستراتيجية والمتقدّمة

المحتويــات

القسم الثالث
قضايا التقنية

تقديــم

سلسلة كتب التقنيات الاستراتيجية
مبادرة الملك عبد الله للمحتوى العربي

يطيب لي أن أقدم لهذه السلسلة التي جرى انتقاؤها في مجالات تقنية ذات أولوية للقارئ العربي في عصر أصبحت فيه المعرفة محركاً أساسياً للنمو الاقتصادي والتقني، ويأتي نشر هذه السلسلة بالتعاون بين مدينة الملك عبد العزيز للعلوم والتقنية والمنظمة العربية للترجمة، ويقع في إطار تلبية عدد من السياسات والتوصيات التي تعنى باللغة العربية والعلوم، ومنها:

أولاً: البيان الختامي لمؤتمر القمة العربي المنعقد في الرياض 1428هـ 2007م الذي يؤكد ضرورة الاهتمام باللغة العربية، وأن تكون هي لغة البحث العلمي والمعاملات حيث نص على ما يلي: (وجوب حضور اللغة العربية في جميع الميادين، بما في ذلك وسائل الاتصال، والإعلام، والإنترنت وغيرها).

ثانياً: «السياسة الوطنية للعلوم والتقنية» في المملكة العربية السعودية التي انبثق عنها اعتماد إحدى عشرة تقنية إستراتيجية هي: المياه، والبترول والغاز، والبتروكيميائيات، والتقنيات المتناهية الصغر (النانو)، والتقنية الحيوية، وتقنية المعلومات، والإلكترونيات والاتصالات والضوئيات، والفضاء والطيران، والطاقة، والمواد المتقدمة، والبيئة.

ثالثاً: مبادرة الملك عبد الله للمحتوى العربي التي تفعِّل أيضاً ما جاء في البند أولاً عن حضور اللغة العربية في الإنترنت، حيث تهدف إلى إثراء المحتوى العربي عبر عدد من المشاريع التي تنفذها مدينة الملك عبد العزيز للعلوم والتقنية بالتعاون مع جهات مختلفة داخل المملكة وخارجها. ومن هذه المشاريع ما يتعلق برقمنة المحتوى العربي القائم على شكل ورقي وإتاحته على

شبكة الإنترنت، ومنها ما يتعلق بترجمة الكتب الهامة، وبخاصة العلمية، مما يساعد على إثراء المحتوى العلمي بالترجمة من اللغات الأخرى إلى اللغة العربية بهدف تزويد القارئ العربي بعلم نافع مفيد.

تشتمل السلسلة على ثلاثة كتب في كل من التقنيات التي حددتها «السياسة الوطنية للعلوم والتقنية». واختيرت الكتب بحيث يكون الأول مرجعاً عالمياً معروفاً في تلك التقنية، ويكون الثاني كتاباً جامعياً، والثالث كتاباً عاماً موجهاً إلى عامّة المهتمين، وقد يغطي ذلك كتاب واحد أو أكثر. وعليه، تشتمل سلسلة كتب التقنيات الاستراتيجية والمتقدمة على ما مجموعه ثلاثة وثلاثون كتاباً مترجماً، كما خصص كتاب إضافي منفرد للمصطلحات العلمية والتقنية المعتمدة في هذه السلسلة كمعجم للمصطلح.

ولقد جرى انتقاء الكتب وفق معايير منها أن يكون الكتاب من أمهات الكتب في تلك التقنية، ولمؤلفين يشهد لهم عالمياً، وأنه قد صدر بعد عام 2000، وأن لا يكون ضيِّق الاختصاص بحيث يخاطب فئة محدودة، وأن تكون النسخة التي يترجم عنها مكتوبة باللغة التي ألّف بها الكتاب وليست مترجمة عن لغة أخرى، وأخيراً أن يكون موضوع الكتاب ونهجه عملياً تطبيقياً يصبّ في جهود نقل التقنية والابتكار، ويساهم في عملية التنمية الاقتصادية من خلال زيادة المحتوى المعرفي العربي.

إن مدينة الملك عبد العزيز للعلوم والتقنية سعيدة بصدور هذه المجموعة من الكتب، وأود أن أشكر المنظمة العربية للترجمة على الجهود التي بذلتها لتحقيق الجودة العالية في الترجمة والمراجعة والتحرير والإخراج، وعلى حسن انتقائها للمترجمين المتخصصين، وعلى سرعة الإنجاز، كما أشكر اللجنة العلمية للمجموعة التي أنيط بها الإشراف على إنجازها في المنظمة وكذلك زملائي في مدينة الملك عبد العزيز للعلوم والتقنية الذين يتابعون تنفيذ مبادرة الملك عبد الله للمحتوى العربي.

الرياض 20/ 3/ 1431 هـ
رئيس مدينة الملك عبد العزيز للعلوم والتقنية
د. محمد بن إبراهيم السويل

مقدمة المترجم

يتجه المجتمعُ نحو ما نطلق عليه صفةَ مجتمع المعرفة، كما يتحولُ الاقتصادُ في العالمِ إلى اقتصادٍ يقوم على المعرفة. ويَنتُجُ من ذلك أن المعرفةَ أصبحت هي الثروةَ وهي الأصول غير المادية في هذه الثروة. والمعرفة تولِّدُ وتخزَّنُ وتنقلُ وتنشرُ وتستثمرُ. أما الأداة في هذا كلِّهِ فهي تقنية المعلومات والاتصالات. وللحفاظ على هذه الثروة وتنميتها لابد من الاهتمام بأمنها. يعالجُ هذا الكتاب أمنَ المعلومات، وبالتالي أمنَ المعرفة أيضاً. يأخذ هذا الموضوع أبعاداً شتى ويدخل في حياتنا اليومية لتعاملنا اليومي مع المعلومات ومع المعرفة.

كَتَبَ هذا الكتاب خمسةٌ من الخبراء الممارسين في هذا الموضوع في حقول الاقتصادِ والتعليم والدفاع والأمنِ والسياسةِ والتقنيةِ والمال. ويتوجهُ الكتابُ لغير الاختصاصيينَ، ويحاوِلُ تَجنُّبَ الغوص في النواحي التقنية المعقدة لهذا الموضوع، ولكنه يحيط بكل أبعاده. يخاطب الكتاب المدراء في القطاعين العام والخاص، كما يخاطب العامة ممن يستعملون الحواسيب والشبكات. ويُعرِّف بمصطلحات هذا الحقل وأسسه الهامة ومبادئه على شكل نصائح وإجراءات يجب أن ينتبه لها الكلّ في القرن الحادي والعشرين.

إن أمن تقنية المعلومات أصبح بالغ الأهمية على صعيد الأفراد والمؤسسات والدول. كما يمس كافة أنشطة حياتنا الاقتصادية والاجتماعية والثقافية والسياسية والعسكرية والعلمية. يبين الكتاب أبعاد الموضوع التخطيطية والإدارية والتقنية والتنظيمية والبشرية. ينتهي كل فصل من فصول الكتاب بجدول نصائح يلخّص الإجراءات المطلوبة. ويشتمل الفصل السابع والأخير على لوائح غنية بالمراجع التي يمكن العودة إليها للاستزادة والتعمق.

لقد حاولت في ترجمة مصطلحات الكتاب، وهي عديدة نظراً إلى حداثة

هذا العلم، أن أشكل حقولاً دلالية نتجنب فيها استعمال نفس المصطلح العربي لأكثر من مصطلح أجنبي. فهناك القرصان والمخترق والكاسر والمتلصص والمتنصت والمقتحم والمعترض والمتطفل والمشمشم، والشركة والمؤسسة والمنظمة والوكالة، والحماية والأمن والسِّرية والتأمين والخصوصية والوثوقية والسلامة، والدخول والنفاذ والوصول، والتزوير والتلاعب والتلفيق والانتحال والاختطاف والسرقة والأذى والاحتيال والجريمة، والتحديث والتحسين والمواءمة والترقيع والتحيين، والحوكمة والإدارة والسيطرة والضبط والتحكم والهيكلة والإجراء والآلية، والمهددات والمخاطر والثغرات والتحديات والخلل، والمعايير والمواصفات والقواعد والقوانين، والتفحُّص والتفتيش والمراقبة والتحقُّق والتفقُّد والتحرِّي والتبيُّن والتقييم والتدقيق، والحاسوب المخدِّم والمضيف والموجِّه والمرشِّح، والقياس والتكميم والحساب، والمنهجية والمقاربة والطريقة وإطار العمل والمنظور، وهكذا.

لقد أضفت بعض الحواشي إلى شرح فقرات قد تكون غامضة أو خاصة بحالة الولايات المتحدة، إذ كانت أكثر الأمثلة التي أتى بها مؤلفو الكتاب من التجربة الأمريكية. كما أضفت في آخر الكتاب لائحة بالمختصرات الإنجليزية مع شرحها بالعربية، وكذلك ثبت بالمصطلحات الإنجليزية مع مقابلاتها العربية وبالعكس. هذا وقد وضع فهرس الكتاب باللغتين أيضاً.

وهنا أقدّر جهود مدينة الملك عبد العزيز للعلوم والتقنية، والمنظمة العربية للترجمة في تبنّي هذا المشروع الرائد والهام، الذي ينقل إلى العربية أمهات الكتب الحديثة في تقنيات استراتيجية ستشكل لبنة من لبنات التوجه نحو مجتمع واقتصاد المعرفة العربي وتساهم في زيادة المحتوى العربي المفيد والبنَّاء.

في الختام، أودّ أن أشكر الآنسة فرح مراياتي التي ساعدتني في الترجمة، وكذلك عمر مراياتي الذي وفّر علي الكثير من الوقت والجهد في طباعة أجزاء من الكتاب.

الرياض في 15/ 3/ 2011
الدكتور محمد مراياتي

تمهيـــد

إن التزايدَ اليومي في تكرار وتعقيد الهجمات المدبَّرة على الشبكة، يؤثرُ في الأنظمة والبيانات وفي دخول المستخدمِ فعلياً إلى موقع كل مؤسسة أعمال أو منظمة حكومية.

سواء أحدثت مصادفةً من قبل مستخدمين عندما يفتحون بريدهم الالكتروني اليومي، أو من قبل هجمة «الحرمان من الخدمة» المدبرة التي تجند عادةً ألفاً من أنظمة «الزومبي»، فان على مديري إدارة تقنية المعلومات ومدراء الشركة أن يكونوا جاهزين للردِّ، وذلك لإبطال التهديدات التي تؤثر في توليد الربح وتسبب العمليات المزعجة لمستخدمي تقنية المعلومات عامة. قد يؤثر قرار أمن المعلومات، التي تمثل ممتلكات أو أصول غير مادية، في العديد من الحالات، تأثيراً مادياً في موازنة الوكالة أو الشركة، وفي الاستثمار المخطط والربح المتوقع للمساهمين.

إن هذا الكتاب موجَهٌ إلى كبار الإداريين ولكلٍّ من يتعامل مع المعلومات، وقد كُتِبَ من قبل مدراء مرموقين، وُنقِّح من قبل إداريٍّ رفيع المستوى في تقنية المعلومات، مع مساهمات من خبراء من الصناعة ومن الحكومة.

قُسِّم الكتابُ إلى ثلاثةِ أقسام رئيسية تتعلق بمنظومة أمن المعلومات ألا وهي: نواحي الحوكمة أو الإدارة، ثم النواحي الهيكلية، وثالثاً النواحي التقنية، متجنباً المصطلحات التقنية المعقدة إلا عند الضرورة. يقدّم كلّ قسم من هذه الأقسام الثلاثة نظرةً شاملةً تتضمن المحاور القانونية البشرية والمالية والاتصالاتية والمخاطر المحيطة واستراتيجيات الإدارة والمحاور التقنية لحماية أنظمة الاتصالات وحواسيب تقنية المعلومات.

لقد وُضعَ **إطارٌ** أو جدول في نهاية كل فصل لمساعدة الإدارة في اتخاذ القرار بشأن التوازن أو الموازنة بين: الاستثمار والأمن والنفاذ إلى المعلومات والالتزام بالقانون. وتوجد في نهاية الكتاب قوائمُ مرجعية لمصادر معلومات متاحة للعامة مرتبطة بأمن تقنية المعلومات.

يمكن للإداريين ومدراء الشركات التنفيذيين أن يختاروا نشاطات الدعم والاستثمارات قصيرة وطويلة الأمد المطلوبة لأمن بناهم التحتية الحاسوبية، مستخدمين في ذلك هذه **الأطر** أو الجداول الموجودة في نهاية فصول الكتاب لاتخاذ قرارات أفضل. تصف هذه الأطر، المبتكرة لاتخاذ قرار الموازنة، الإجراءات والأعمال التي تحمي بفاعلية النفاذ إلى النظم والمعلومات في عالم التحدي والتغير السريع، وذلك من خلال تقديم أفضل ممارسات محترفي تأمين المعلومات ومستشاري الأمن في الحكومة والصناعة.

يناقش **فصل النظرة التنفيذية الشاملة** مفهوم الأمن كعملية، وهو مفهوم قد أكسب اهتماماً خاصاً داخل مجتمعات الأمن وتقنية المعلومات. تتضمن المواضيع العديدة، التي استعرضها الفصل، العالم الجديد لأمن تقنية المعلومات، والقيمة المتزايدة باستمرار لممتلكات (أصول) المعلومات، ومسؤوليات وتحديات الأمن أمام الإدارة العليا ورؤساء المؤسسات اليوم.

يستعرض **القسم الأول قضايا الحوكمة** في أمن تقنية المعلومات، بما فيها مسألة الموازنة بين خصوصية الموظف والنفاذ إلى المعلومات، وسياسات الأمن الإدارية، والنواحي القانونية، واستراتيجيات إدارة المخاطر والوثوقية بالأنظمة المعتمَدة.

يطرح **القسم الثاني قضايا هيكلة منظومة أمن تقنية المعلومات،** وذلك ابتداءً من بناء مصفوفة التهديد. يزوّد القسم بعد ذلك تفاصيل حول ملاءمة الهيكلية مع اتفاقيات مستوى الخدمة، ومع إنشاء حواجز الحماية متعددة المستويات، ومع كشف التهديدات الداخلية لعمليات أمن تقنية المعلومات. يناقش القسم أيضاً منهجيات التخطيط لتجنب الكوارث.

يركّز **القسم الثالث على قضايا تقنيةٍ** تتداخلُ معَ، وتدعمُ قضايا الحوكمة وقضايا النواحي الهيكلية. تستحوذ مقومات التقنية على نسبة كبيرة من استثمارات أمن تقنية المعلومات ويحتاج الإداريون فهم كيفية تطبيق التقنية،

وكيفية عملها، وسبب الغلاء الكبير لتشغيلها وصيانتها. يستعرض هذا القسم حماية برمجيات COTS، ونظام حفظ واسترجاع البيانات، والتخطيط للاستمرارية، وتقادم البيانات، والمميزات البيولوجية في التحقق من الهوية، والبطاقات الذكية، وتخزين المعلومات، واختبار اختراق أمن المعلومات.

تُعَدُّ مراجع مواد الكتاب مؤشرات لمصادر أمن المعلومات المتاحة علانيةً. وبما أن هناك تطورات كبيرة متوقعة في المبادئ التقنية والتشريعية في السنوات المقبلة، فإن العودة دورياً إلى هذه المراجع بدافع التحديث لأمرٌ صائب ونافع.

كلمة شكر

إن كتب التقنية والأمن عبارة عن مساهمات جماعية من وجهتي النظر الإدارية والتقنية.

لقد حَظِيَ كتاب **أمن تقنية المعلومات: نصائح من خبراء** بتنقيحات تحرير، وبمساهمة من الكثير من خبراء هذا المجال، الذين أعطوا بسخاء من وقتهم ومعرفتهم.

إن الأشخاص الآتي ذكر أسمائهم قد قدّموا إسهامات في هذا الكتاب أو نقّحوا جميع أجزائه أو جزءاً منه:

روبرت ل. لوري، مدير سابق لخدمات التصميم بمساعدة الحاسوب، في شركة تي آر دبليو TRW المحدودة ـ نورمان ج. شويتزر، كبير مدراء شركة CATIA المحدودة ـ دوغلاس بيورفانس، مسؤول ورئيس الإدارة التنفيذية، شركة التجارة العالمية الالكترونية ـ جون ويبل، كبيرمدراء المشروع، شركة ديل للحواسيب Dell ـ دوروثي نولان، مسؤول ورئيس الإدارة التنفيذية لشركة أوفيكس ـ غوردون كاستيان، مسؤول ورئيس الإدارة التنفيذية في شركة سباين العالمية ـ تيموثي سلوسر، نائب الرئيس، القطاع الفيدرالي سي إس سي ـ كيفن كيللي، مسؤول البر امج في برنامج التحالف «برايم» ـ آرون فيلبس، مدير اختبار النظام والعمليات ـ تيد بريم، مدير مشروع ام اي اف ـ جون مكينا، مدير عمليات هندسة الأنظمة، برنامج التحالف «برايم» ـ ستيفن بروكتور، نائب المدير، برنامج التحالف «برايم» لهندسة البنية التحتية ـ ريتشارد فوشت، مدير مكتب الخصوصية والحماية، برنامج التحالف «برايم» و جون بولينس، مدير هندسة البنية التحتية، برنامج التحالف «برايم».

لهؤلاء الأشخاص ولأخرين قد أكون قد أخفقت في إعطائهم الثناء الذي يستحقون: لقد كانت أفكاركم واقتراحاتكم وإرشاداتكم، طيلة سنوات، قيِّمة

للغاية وتقدّر إلى حدّ بعيد. إن أيّ خطأ أو إغفال هو بالطبع من اقتراف يدي. أرجو إعلامي بالأخطاء عبر البريد الالكتروني (IITSbook@aol.com) وسوف أبذل قصارى جهدي لتصحيح الأخطاء المطبعية في النسخ المعدلة التالية للكتاب.

يتوجبّ عليّ أيضاً التعبير عن شكري للمساهمين الرئيسيين الأربعة في هذا الكتاب: كريسان هيرود، تشارليز ريكس، كليفتون بوول، وكريج إي. كوشر. لقد كانت نوعية المحتوى الذي قدّموه والتزامهم بالمواعيد غاية في الدقة، وذلك على الرغم من المسؤوليات العظيمة تجاه وظيفتهم الطبيعية في جامعة الدفاع الوطني في مقاطعة واشنطن.

من وجهة نظر الإدارة العليا، ستكون التغيرات في مستقبل أمن تقنية المعلومات محبطة ومرضية على حدٍّ سواء. فمع كل يوم تظهر سلسلة من التقارير والمتطلبات مفصّلةً خروقاً أمنيةً ورقع برمجيات وثغرات. إنه لأمر محبطٌ لكلا محترفي الأمن والهيئة الإدارية التنفيذية، أنه مهما طُوّرت الأساليب الدفاعية واشُتريت وثبتت أو شُغلت، فإنها سوف تُخرق أو تُهزم مع الوقت من قبل أُناسٍ أذكياء أو من قبل مقومات التقنية التي يساء تطبيقها.

من ناحية أخرى، إن النجاح في منع الأشخاص المحظورين والهجمات الاقتحامية من التأثير في المعلومات والأنظمة والشبكات والأبنية كل يوم، وكذلك النجاح في استمرار عمل المؤسسة بدون توقف، هما أمران يفتخر بهما حِرَفِيّاً. إن الهدف بالطبع هو تحقيق نجاح مؤكد 100٪ في أمن المعلومات وفي الأنظمة والشبكات ـ لكنه عمل صعب ومليء بالتحدي.

متمنياً لكم النجاح الدائم في حماية ممتلكات (أصول) أنظمتكم وشبكاتكم ومعلوماتكم أربعاً وعشرين ساعة على مدار الأسبوع.

لورنس م. أوليفا
ريستون، فيرجينيا
شباط/ فبراير 2004

الفصل الأول

نظرة تنفيذية شاملة

لورنس م. أوليفا

العالم الجديد الدائم لأمن تقنية المعلومات

إن اجتماع العديد من الأحداث المرتبطة ببعضها البعض، بما في ذلك اتساع التطبيقات غير المحمية المتصلة بالإنترنت، والحرب الشاملة على الإرهاب العالمي، والتأثيرات المالية الكبيرة لسرقة الهوية والمعلومات، جعل من أمن تقنية المعلومات عنصراً جوهرياً لمعظم خطط تقنية المعلومات الحكومية والخاصة.

يقوم مثالان اثنان خلال عام 2003م بشرح نطاق مشكلة الأمن وكلفته، حيث: ازدادت الاعتداءات على شبكات الاتصال الالكترونية cyber بنسبة 40٪ في الفصول الثلاثة الأولى من السنة، وقُدِّرت تكلفة تطهير الهجمات المتعددة للفيروس و«الدودة» أثناء صيف ذلك العام بنحو 3.5 بليون دولار، وذلك وفقاً لمركز التنسيق CERT، وهو مركز مراقبه حماية شبكات الاتصال الالكترونية.

لقد اتسعت استراتيجيات الأمن الداخلية نظراً إلى تشابك عوامل الوثوقية والأداء والمقدرة، وتجاوزت موضوع إبقاء قراصنة الإنترنت والمتطفلين بعيداً عن المستخدمين الموثوقين من خلال التحقق من الصفات البيولوجية للمستخدم وعوامل أخرى، ومن خلال تعقب الدخول المباح داخل ما يسمّى بـ «جدران النار» من قبل مستخدمي النظام، ومن خلال التحليل الكاشف للبرمجيات

المدمرة. وعلى أية حال، إذا ما أخذنا بعين الاعتبار القيود الاقتصادية الموضوعة على نفقات الشركة، فإن الجهود المبذولة في أمن المعلومات كانت غالباً قليلة جداً ومتأخرة جداً لتوقف المخترقين المصممين من تحقيق الوصول إلى أصول المعلومات.

إضافة إلى التعقيد التقني لموضوع أمن المعلومات، توجد قضايا قانونية تتعلق بخصوصية المستخدم، وقضايا المسؤولية القانونية حيال ضمان عدم سرقة سجلات ومعلومات الزبون، والالتزام الحكومي بالقوانين مثل(*) HIPAA,GLBA,FCRA,NORPDA,PIPEDA,SAFTEY, SARBANESOXLEY and the (U.S.A PATRIOT Act).

من جهة أخرى، فهناك، إضافة إلى العمليات والخطط طويلة الأمد، نشاطات آنية مباشرة لمجابهة الهجمات الواسعة على النظام والشبكة تقوم بها برمجيات خبيثة (تدعى Malware) مثل الديدان، والفيروسات، وأحصنة طروادة وأنظمة «الزومبي».

ونظراً إلى أن وثوقية التقنية الحديثة قد رَفَعت من توقعات المستخدم إلى تَطلُّب وجود الخدمة أربعاً وعشرين ساعة على مدار الأسبوع، فإن مستوى التعقيد الإداري المتعلق بتلك الدرجة من الخدمة قد تطلب استثمارات أوسع في التجهيزات، وعدد موظفين أكبر، ووعي بالغ لنتائج كلّ قرار يُتَّخذ فيما يتعلق بأمن تقنية المعلومات.

لقد أُجبرَ مدراء ومنفذو تقنية المعلومات حكماً على أن يصبحوا خبراء ـ مع المسؤوليات المقترنة بذلك ـ في مواضع مختلفة عديدة خارج مجتمع تقنية المعلومات التقليدي.

إن هذا المستوى المضاف في تعقيد الإدارة قد اعتُرِفَ مؤخراً بأهميته وتأثيره في مجتمع تقنية المعلومات نظراً إلى ضغط مواعيد الإنتاج والتسليم المحددة. لقد جرى إقرار العديد من القوانين المؤثرة بشكل غير مباشر في مجتمع تقنية المعلومات منذ 11 أيلول/ سبتمبر 2001. ولا يزال تأثير هذه التغيرات يحدد من قبل رجال الصناعة ورجال القانون، وما يترتب على ذلك من نشاطات التدريب

(*) هذه مختصرات لقوانين صادرة في الولايات المتحدة تتعلق بأمن المعلومات، وسيأتي ذكرها لاحقاً في فصول الكتاب.

المطلوبة لتحقيق الوعي الكامل والالتزام من قبل كل الجماعات المتأثرة. على أية حال، فإنه لأمر واضح بأن أنشطة أمن الأنظمة وأصول المعلومات ستحتاج إلى الزيادة زيادةً كبيرةً كي تستجيب لهذه القوانين الجديدة، وإلاّ فإن المنظمات والمؤسسات ستتحمل غرامات مالية واتهامات قانونية بالتقصير.

الأمن بوصفه عملية

لم يعد أمن تقنية المعلومات مجرد حدث أو مهمة مؤقتة بالنسبة إلى المنظمات الحكومية والخاصة. لقد أصبح عملية مستمرة في كلّ ثانية من كلّ يوم من وجهةِ النظرِ التقنيةِ والإدارية. إن معظمَ المدراءِ التنفيذيين في الشركات الصغيرة لا يزالون غيرَ مدركين أن «جدار النار» الخاص بشركتهم يُسبَرُ مئات المرَّاتِ في اليوم من قبل أدوات السطو الآلية. كما تُسبَرُ «جدران النار» الحكومية وتلك الخاصة بالخدمات المالية غالباً عشرات آلاف المرات كل يوم.

إن أدوت السطو هذه ـ والعديد منها متوفر مجاناً عبر الإنترنت يمكن أن توظف ضد ملايين الأنظمة بضغطات قليلة من الماوس (الفأرة). وحالما تجد هذه الأدوات نظاماً غير محمي، أو نظاماً محمياً بشكل رديء، تقوم بتسجيل عناوين الـ IP (بروتوكول الإنترنت) ومعلومات أخرى مفيدة للقراصنة والمخترقين في استغلال النظام أو الشبكة للحصول على بيانات قيمة. يمكن للقراصنة أيضاً أن يحوّلوا النظام إلى نظام «زومبي»(*) أو الحرمان من الخدمة (DoS) لإغراق الأنظمة المستهدفة بملايين الرسائل وإضعاف قدرتهم على معالجة المعلومات المباحة ونقلها.

تشتمل إجراءات الأمن القوية على طبقات عديدة للوظائف التشغيلية بما فيها التالي:

- نقاط داخلية وخارجية للسيطرة على النفاذ أو الدخول إلى النظام مثل «جدران النار» (من تقنيات أمن المعلومات)
- تَحَقُّقٌ قوي من هوية المستخدم عند طلبه النفاذ أو التحميل.

(*) تستعمل برامج حاسوبية خبيثة للسيطرة عن بعد على حاسوب مستهدف وجعله يأتمر بأوامر القرصان، ويسمى عندها الحاسوب المستهدف «الزومبي» أي الجثة المسيَّرة.

- مراقبةُ وتسجيلُ النفاذ إلى كلٍّ من شبكة المستخدم، والنظام، والمعلومات.
- تطبيقُ عمليات تعميةِ (تشفير) البيانات، كلما كان ذلك ممكناً.
- استخدامُ شركاءَ معتمدين موثوقين عند تبادل البيانات.
- التنصيبُ الفوري لرُقَعِ البرمجيات المتوفرة حالياً.
- تدريبُ المستخدمين الخارجيين والداخليين على أجهزة التحكم بكلمة المرور وبالنفاذ المحظور إلى المعلومات.
- الأمنُ المكاني لغرفِ التجهيزاتِ وأنظمةِ استرجاع بيانات البرمجيات، ووثائق المعلومات المطبوعة.
- سياساتُ إدارةِ الاستخدام المسموحِ والمحظور، ومراقبة الإدارة، ومتطلبات خصوصية المستخدم.
- عمليةُ تحليل السبب الرئيسي وراء «ما حدث» عندما تقع الأحداث غير المتوقعة.
- خطةٌ شاملةٌ وآمنةٌ لاستعادة الخدمة والمعلومات يمكن إطلاقها فوراً عندما تقع الكارثة.
- سلسلةُ هرمِ المسؤولية الإدارية لكبح المشاكل الصغيرة سريعاً، ولتخصيص الموارد لحل المشاكل الأكبر بسرعة.

تبنى هذه الطبقات فوق بعضها البعض تدريجياً وبشكل متعاضد لخلق بنية الأمن. على سبيل المثال: تستطيع سياسةٌ قويةٌ للتحقق من الهوية مَنعَ المستخدمين المجهولين من تحقيق النفاذ إلى الشبكات والأنظمة، أمّا المستخدمون المعروفون فيستطيعون الدخولَ وإنجازَ عملهم مع وجود نظام رقابةٍ وتفتيشٍ آليٍّ حول ما قاموا بعمله ومتى قاموا به. تُقبلُ البياناتُ من المصادرِ الخارجية الموثوقة فقط لمنع تلوث قواعد البيانات بمعلومات محرّفة بشكل واضح (أو أسوأ من ذلك بمعلومات نصف صحيحة).

قيمةُ أصولِ المعلومات

تُشكِّلُ المعلومات قيمةً لمالكيها ولمستخدميها ولأنظمتها الآلية التي يفترض أن تستخدمها وللوكالات الحكومية التي تنظمُ النفاذَ إليها. فعلى سبيل

المثال: لم تكن مخازن Wal-Mart(*) لتستطع العمل بفعالية لولا إنشاؤها مستودعَ بيانات بسعة 30 تيرابايت يُتابعُ التكلفة، والربح، والمدة الزمنية لتخزين المنتج، وحسابات أخرى متعلقة بكل منتج تمّ بيعه، وذلك في كلِّ مخزنٍ، خلال السنوات الخمس الماضية.

ما كان لشركات الطيران العالمية والمحلية الرئيسية أن تستطيع أن تجدول وتقوم بملاحة الطائرات ببلايين الدولارات بشكل فعّال، ولا أن تُشغِّلَ نماذج تعظيم دخلهم، لولا استخدامهم قواعد بيانات معقَّدةٍ وأنظمةِ المعلومات التي تقدَّرُ تكلفة استبدالها بأكثر من عدة بلايين من الدولارات.

إن خطَّةَ عمل بطاقات الفيزا، وانترناشونال كارد ماستر، وأمريكان اكسبريس، تبنى حول جَمع بياناتِ استخدام البطاقة، ومتابعةِ الحسابات، وتحليل الغش، وإرسال الفواتير للزبون، ومعلومات استلام المبلغ، وذلك كله من أجل مئات الملايين من بطاقات الائتمان والشراء. إن القيمة الإجمالية لقواعد بيانات هذه الشركات وأصولِ معلوماتهم تقدر بمئات البلايين من الدولارات ـ أكثر من الميزانيات السنوية لجميع دول العالم باستثناء الولايات المتحدة الأمريكية واليابان.

إن المؤسسات التجارية، المشاركة في سوقِ المالِ وفي المنشآت المالية، لن تكون قادرةً على فتحِ أبوابها ما لم تملك الثقة بدقة المعلومات المستخدمة في إدارة المؤسسة ومعرِفة قيمتها وتقدير الأرباح العائدة منها. فالمعلوماتُ الدقيقةُ والموثوقة هي دعامةٌ مركزية لشفافية السوق وثقة المستثمر.

من أين تستمد المعلومات قيمتها؟ جزيئاً من كونك قادراً على الاستفادة منها كثيراً من أجل تحقيق فوائد ماليةٍ وتحليليةٍ وإداريةٍ واجتماعيةٍ وتشغيلية. تزداد قيمة المعلومات عندما تُجمعُ وتُثبتُ كمعلومات دقيقه، وذلك في كل مرة تحدث فيها عملية تجارية ناجحة أو استخدام ناجح، ويتراكم تزايد هذه القيمة لأن كل عملية تجارية ناجحة تؤدي إلى عملية تجارية ثانية وبعدها ثالثة، . . . الخ، طوال الوقت. فالصفقةُ الواحدّةُ ببيع مئة سهم على سبيل المثال يمكن أن تتسبب بصفقات شراء أسهم أخرى، وبصفقاتٍ لبضائع رأسمالية مثل السيارات، أو الشاحنات، أو الطائرات، أو الممتلكات، والتي مع مرور الوقت

(*) وهي كبرى محلات التجزئة الأمريكية.

ستطلق صفقات لموجودات أخرى، ولصيانة وحفظ المركبات والممتلكات، ولتوظيف كوادر بشرية. تفيد المعلومات الدقيقة، عندما ينظر إليها من الناحيتين المالية والتجارية نظرة شمولية من البداية إلى النهاية، في الحصول على الكسب المالي القائم على التعاملات أو الصفقات، وعلى الاستفادة من التسويق، وعلى اتصالات الزبون المباشرة وعلى الشراكات التعاونية التي ستكون معقدة أو غاليةَ التأسيسِ بدون هذه المعلومات.

تبلورت الفكرة التي تقول بأن للمعلومات قيمة كبيرة من قبل الدكتور ديفيد نولان في مقالته في مجلة *Harvard Business Review* في عام 1982 (Nolan, 1982)، ونُقِّحَت من قبلِهِ ومن قبلِ آخرين منذ ذلك الحين. قدم نولان عام 2001 الفكرة القائلة بأن قيمة أنظمة المعلومات، بالنسبة إلى المنظمات، تزداد عبر سلسلةٍ من «مراحل» تطور التقنية ابتداءً من عهد الحاسوب المركزي الضخم عام 1960 إلى عام 1980 إلى عهد الحاسوب الصغير من عام 1980 إلى عام 1995 وإلى عهد الشبكة (الإنترنت) اليوم. إن القدرة على توسيع استخدام المعلوماتِ لأغراضٍ نافعةٍ، وغير متوقَّعةٍ أحياناً، تَنتجُ من التغيراتِ التقنية. ذكَر نولان بأن مايكروسوفت استخدمت الإنترنت لتتفاعل مع 400,000 زبون لتجريب نسخة «بيتا» من برمجيات «ويندوز 95». إن الاستجابة للملاحظات المستلمة من هؤلاء المستخدمين قد مكّنت مايكروسوفت من إعادة تصميم وتوضيح كيفية عمل المنتج قبل إطلاقه الأخير في السوق. إن تَوفُّرَ إمكانية استخدام الإنترنت كنظام توزيع، وكوسيلة اتصالات بالزبائن، وكذلك توفر أنظمة تعقبٍ متكاملةٍ، قد أتاح لشركة مايكروسوفت اختبار نسخة «البيتا» من قبل مئات الآلاف من الأشخاص ـ في حين تضمنت تجربة الإصدارات السابقة نسبة ضئيلة من الزبائن، وبالتالي لم تحظَ ببيئةِ اختبارٍ متعددةٍ كالتي حظيَ بها نظام ويندوز 95.

بينما يتفق معظم كبار المديرين والمدراء التنفيذيين على أن المعلومات تملك قيمة فعلاً، إلا أنهم غالباً ما يحسبون هذه القيمة على أساس تكلفةِ جَمعِها وصَونها وإدارتها، بدلاً من القيمة المتوقعة التي ستكسبها المنظمة من خلال الاستفادة من المعلومات لتحقيق أهداف الشركة ودعم حاجات زبائنها بطرق غير مخطط لها مسبقاً. فعلى سبيل المثال: تستخدم الآن شركتي «كيت وي» و«ديل»(*) (هما في

(*) Gateway and Dell وهما من كبرى شركات الحاسوب.

الأصل مصنعي حواسيب شخصية) قواعد بيانات الزبون الضخمة لديهم، لتسويق شاشات تلفزة البلازما، والمنظمات الرقمية الشخصية، ومشغلات الموسيقى الرقمية، ومنتجات أخرى لم يُخطَّط لها في نماذج عملهم الأصلية.

هدف العديد من مبادرات الحكومة الالكترونية، منذ عام 1996، إلى توسيع قيمة المعلومات الحكومية المتراكمة وزيادة الاستفادة منها، فعلى سبيل المثال، لقد أُنشئ العديد من البوابات على شبكة الإنترنت من قبل الحكومة الفيدرالية للولايات المتحدة لإتاحة وصول المواطنين إلى معلومات مثل: إعادة مال الضريبة، وفرص التعاقد، ومعلومات حجز مواقف السيارات، ومعلومات إجازات وتراخيص السواقة، ووضعية التشريعات قيد الإعداد، والبيع والتوزيع الالكتروني للمنشورات الحكومية، والعديد من الخدمات الأخرى. إن إدراك إمكانية تحويل التعاملات الحكومية إلى تعاملات إلكترونية، قد أدى إلى الانتفاع من قواعد البيانات الحكومية عن طريق بوابات نفاذ متوفرة طيلة 24 ساعة وعلى مدار الأسبوع بدون زيادة التكاليف الثابتة التقليدية من موظفين ومكاتب وأنظمة اتصالات.

قد تملك الشركات والمنظمات الصغيرة أيضاً قيمةً كبيرةً في المعلومات التي لدى شركائهم وزبائنهم، فبإمكان صانعي السلع والخدمات الفريدة، أو مزوديها، أن يستفيدوا من المعلومات حول أولويات الزبائن أو احتياجاتهم لخلق أسواق جديدة للشركة، كما فعلت شركتا «ديل» و«غيت وي». وقد تدمج المعلومات، بعد جمعها والتأكد منها لهدف معين، مع قواعد معلومات الآخرين المتوفرة تجارياً وذلك لمعرفة توجهات السوق مع الزمن ولمعرفة فرص تسويق منتج من فرص منتج آخر. على سبيل المثال: قد يشتري صانعو البيانو قاعدة معلومات من صانع جهاز تسجيل الصوت عالي الدقة ليروا ما إذا كانت الزبائن ترغب بتسجيل معزوفاتهم الموسيقية. يهتم صانعو بطاريات آلات التصوير الرقمية والهواتف النقّالة كثيراً في قواعد بيانات الزبائن المتوفرة لدى مخازن آلات التصوير وشركات الخليوي. إن شركات التأمين التي تمنح «بوليصات» التأمين ضد التخريب والسرقة لهذه المنتجات ستكون مهتمة أيضاً في أيٍّ من هذه المعلومات.

إن الفكرة القائلة بأن للمعلومات قيمة هي فكرة مهمة جداً بالنسبة إلى

الشركات والحكومات. فإذا كانت للمعلومات قيمة ضئيلة (أو لا قيمة لها أبداً) بالنسبة إلى المنظمة التي تقتنيها أو تجمعها، فسيكون هناك مبررٌ ضعيفٌ لتقوم هذه المنظمة بإنفاق الموارد لحمايتها. إذاً فإن القيام بتحديد قيمة معلومات المنظمة هو مسؤوليةٌ إلزاميةٌ بالنسبة إلى المدير التنفيذي أو الإدارة العليا باعتبار أنه يترتب على هذا القرار العديد من الأفعال حول تحديد أو إباحة النفاذ إلى المعلومات، والأنظمة والشبكات. إن المهم ليس تحديد القيمة الدقيقة للمعلومات بل تحديد وجود قيمة (كثرت أو قلّت) تَجِبُ حمايتها من الفقدان أو سوء الاستخدام أو الإفساد.

تحديات ومسؤوليات وأمن المعلومات

مع التزايدِ المستمرّ للتعقيد التقني، والمصاعبِ القانونية، وتوقعاتِ حماية الخصوصية، ارتفعت تحديات أمن المعلومات بشكل متسارع خلال السنوات الخمس الماضية. إن الانتشارَ الكبيرَ، مع نهاية التسعينيات من القرن الماضي، في استعمال التطبيقات المعلوماتية القابلة للعمل مع الإنترنت (web-enabled)، وتزايد حصة هذا الانتشار في سوق الأسهم، غالباً ما دفع بمرتبة عمليات أمن المعلومات إلى مستوى الأفضلية الثاني أو الثالث. يستمر العديد من الأنظمة المالية وواجهات نفاذ المستخدمين للنظم الحاسوبية، التي تحتاج إلى أن تكون محمية بشكل عال، باستخدام كلمات سرٍّ مؤلّفةٍ من ستة حروف، وذلك بسبب الخلاف المستمر ضمن صناعة الحاسوب حول الموازنة بين درجة حرية المستخدم وحماية النفاذ للمعلومات.

إن الجريمة الحاسوبية الانتهازية هي الآن مجرد ضغطةٍ أو ضغطتين على لوحة مفاتيح الحاسوب وهي في متناول أي شخص يستطيع ـ وغالباً يفعل ـ تحميل أدوات قرصنة متاحةٍ مجاناً على شبكة الإنترنت. إن مهندسي أمن المعلومات على دراية بكيفية عمل هذه الأدوات، كما أن الشبكات المحميةِ والمصممةِ بشكلٍ جيدٍ تستطيع عادةً حظر اختراقهم عند المستوى الأول لـ «جدار النار». أما الشبكات التي تبنى بشكل غير صحيح، أو لا تُطبِّقُ آلية دائمة لـ «ترقيع» البرامجِ، أو أنها غير موائمة بشكل مستمر ـ تذكر بأن الحماية عبارة عن عمليةٍ مستمرةٍ وليست حدثاً لمرة واحدة ـ فإنها تُهاجَمُ غالباً بنجاحٍ مع إتلافِ المعلومات أو الحصول عليها بشكل غير شرعي.

تتضمن التحديات التي تواجهها إدارات تقنية المعلمات ما يلي:

1. مَعرفةَ من يمكن له ـ ومن لا يمكن له ـ الوصول إلى المعلومات، والأنظمة والشبكات. فأحياناً قد لا تُبَلَّغُ سجلات الموظفين الدقيقة بسرعة إلى إدارة تقنية المعلومات، أو لا تُحفَظُ على الإطلاق في أحيان أخرى، ممّا يؤدي إلى قرار السماح بالنفاذ (أي) «الترحيب» الخاطئ.

2. عَدَمَ فهم الفرق بين العديد من تقنيات أمن المعلومات المختلفة والمتضاربة أحياناً والمتوفرة من قبل العديد من المزودين.

3. تَرَقُّبَ صدور معايير أمن معلوماتٍ شاملةٍ متفقٌ عليها من قبل جميع المزودين الرئيسيين للشبكة والبرمجيات ومن قبل الحكومة.

4. المحافظةَ على مقدرةٍ هندسيةٍ للاستجابة السريعة ضدَّ الفيروسات، والديدان، وأحصنة طروادة، وهجمات الحرمان من الخدمة (DoS)، بالإضافة إلى التفحُّصِ المستمرِ للشبكةِ وللنفاذ إليها من القراصنة والمخترقين الذين يحاولون الوصول إلى المعلومات القيِّمة.

5. تطويرَ وصيانةَ سجلاتِ إدارةِ هيكليةِ منظومة المعلومات المتعلقة بمستويات «ترقيع» برمجيات أمن المعلومات، وذلك لكلٍّ من الأنظمة الحساسة وغير الحساسة.

6. معرفةَ أين يجب تطبيق «رُقَع» البرمجيات أولاً، من أجل الحصول على أفضل النتائج لتقليل تأثر نظام المستخدم أو نظام الإنتاج بالهجمات، على سبيل المثال: إن أنظمة البوابات الموصولة مع الشبكات العامة هي عادة خط الدفاع الأول، ويجب أن تملك المستويات الأحدث للبرمجيات، مقارنةً، مثلاً، بالنظام المكرس لطباعة بطاقات الترميز بالخطوط على خط إنتاج البضائع.

7. تحديد مستوى النفاذ الصحيح لكلٍّ واحدٍ من الموظفين ومستخدمي النظام ليقوموا بعملهم بدون السماح للجميع بالنفاذ الكامل لجميع الملفات والأنظمة.

8. معرفة من يمكن أن تثق به من المزودين والشركاء والزبائن من أجل تزويدك بالمعلومات. فليست كل المعلومات سواء ـ فقد تحتوي مرفقات البريد الالكتروني على فيروسات أو ديدان، وقد تحتوي الصور على رسائل محشوة

(تعمية معروفه بـ Steganography)، ومن الممكن أن تحتوي الملفات «القابلة للتنفيذ» على «أبواب مفخخة» أو «قنابل موقوتة».

9. جذب مهندسين مؤهّلين في أمن المعلومات واستبقائهم من خلال تحديات شخصية وتعليمية.

10. توفير ميزانيات كافية من أجل مزودي الخدمة والموظفين والأجهزة. إذ إن أمن المعلومات مطلبٌ يوميٌ من متطلبات العمل مثل إبقاء الأضواء مشتغلة والهواتف شغّالة.

تستمر التحديات القانونية بالازدياد مع بداية فهم المحامين لعناصر التقنية والأثر المالي والتشغيلي الذي ينتج من فقدان معلومات قَيِّمة لصالح مستخدمين غير شرعيين. يلام مطورو التقنية والمجهزون ومزودو الخدمة، باستمرار، لعدم تصميمهم أنظمة أو برمجيات آمنة، ولعدم التخطيط لمواجهة جميع سيناريوهات الأمن الممكنة. كما أن إدارة تقنية المعلومات تلام لعدم قيامها بكلّ ما هو ممكن لتوظيف أفضل الوسائل الدفاعية ضد النفاذ المحظور أو فقدان المعلومات. يلام المستخدمون المهملون أيضاً على فقدان أو مشاركة كلمات السِّر، والمعلومات الأمنية، وهوية المستخدم، مخالفين بذلك سياسة المنظمة أو الشركة، وبالطبع فإن القراصنة ـ عندما يعثر عليهم ويتم تحديدهم ـ يعتقلون ويزجون في السجن.

ومع ظهور جرائم الحاسوب الخطيرة بشكل أوسع فأوسع، يتزايد اللوم على الإدارة العليا والإدارة التنفيذية لتقنية المعلومات، وغالباً ما يقال: «كان عليهم أن يعلموا أن حدوث هذا أمر محتمل». وإذا ما أخذنا بعين الاعتبار تزايد سرقة الهوية والمعلومات عالمياً، فإننا نستنتج بوضوح أن من الواجب على إدارة تقنية المعلومات أن تخطط لسيناريوهات الحالة الأسوأ، بالرغم من أنها قد تكون قليلة في العدد.

من ناحية ثانية يجب على الإدارة العليا والإدارة التنفيذية لتقنية المعلومات أن تستبقي على وضعية التيقظ في كل ما يمتّ بصلة إلى أمن المعلومات باعتبار أن أثر الهجمة أو السرقة الناجحة قد يكون فادحاً للزبائن والمنظمة من حيث فقدان ثقة الزبون، والمعلومات غير الموثوقة، ونفقات إصلاح ما حدث.

يُشكِّل التزوير المتعلق بالإنترنت أكثر من 55 ٪ من بين ما يزيد على

500000 شكوى زبائن سجلتها «المفوضية التجارية الفيدرالية الأمريكية» في عام 2003. ووفقاً لهذه الوكالة، يشكل ذلك تزايداً بنسبة تربو على 45٪ عن عام 2002م. تَذكُرُ الوكالةُ أيضاً أن متوسط خسارة ضحايا التلاعب المتعلق بالإنترنت كانت 195 دولار. وكانت سرقة الهوية الرقمية أكثر الشكاوى شيوعاً للسنة الرابعة على التوالي ممثلة 42٪ من جميع الشكاوى في عام 2003 (FTC, 2004).

لسوء الحظ فإن مسؤوليات الفريق التنفيذي لتقنية المعلومات، المتعلقة بالمحافظة على المعلومات الشخصية والمدنية والمشتركة، تستمر بالاتساع من خلال التشريعات الجديدة، وتوقعات قوى السوق، والغرامات التي تفرضها المحاكم. فعلى سبيل المثال: منذ عام 1996 أصدر الكونغرس الأمريكي العديد من القوانين بما فيها: [HIPPA,GLBA,21C.F.R.PART11 (FDA DRUG MUNUFACTURE), Sarbanes-Oxley AND E-SIGN] التي تحدد كيف يجب أن تحمى المعلومات من المستخدمين غير الشرعيين، و/أو كيف يجري ضمان شفافية وصحة المعلومات المعتمدة.

في عام 2003م بدأ قانون «لا تتصل هاتفياً» بالتطبيق مانعاً اتصالات تسويق السلع التي تجري بواسطة الهاتف عن معظم الشركات الخاصة التي ليس لها علاقة قائمة مع الزبون تبرر الاتصال. لقد أقنعت القوى المناهضة لطريقة التسويق عبر الهاتف الكونغرس للتغلب على تحديات القانون الحالية. إن مؤيدي الخصوصية الشخصية مثل الاتحاد والمركز التاليين:

National Law Center و Electronic Frontier Association يراقبون بفعالية أحداث سرقة الهوية، وردود أفعال الشركات حيال اعتماد طرق مبتدعة لإيقاف سرقة المعلومات ذات الخصوصية، ويدعمون مساندة ضحايا هذه الجريمة. إن مؤيدي الخصوصية هؤلاء وآخرون أيضاً مستاؤون مثلاً من الاستخدام المقترح لبرنامج تفحص المعلومات الخاصة بركاب الطائرة المسمّى CAPPS2، الذي يصنف أهم المعلومات حول هوية كل راكب مستخدماً الجمع بين قواعد المعلومات الخاصة والعامة. لقد صرحت مصادر حكومية بأن المعلومات عن الراكب الموجودة في قاعدة بيانات CAPPS سوف تحذف بعد أن تنتهي الرحلة بأيام قليلة، إلا أن مؤيدي الخصوصية لم يبلغوا بتفاصيل ذلك. بدأ بعض ركاب الطائرات برفع دعوى قضائية بشكل مستقل ضد حصول الخطوط الجوية على بياناتهم الشخصية. ولكنه لا يعرف الآن ما هي البدائل القابلة

للتطبيق ـ إن وجدت ـ لعملية التفحص هذه التي تمارسها شركات الطيران.

إنه لأمر محتمل، من وجهة نظر تقنية المعلومات، أن تتم مطالبة الشركات التجارية والمنظمات الحكومية بتزويد معلومات تمس خصوصية الزبون أو الشركة لتستخدم لأهداف التفحص الأمني. ومن المرجح أن الزبائن والشركات سيكونون مستاءين جداً من هذا الوضع، وسيحاولون ممارسة ضغوطات يسمح بها نظام السوق الحر مثل ـ مقاطعة الشركات التي تُسرِّب المعلومات، ورفع الدعاوى القضائية، وتزويد معلومات غير كاملة ـ وذلك لإيقاف انتشارها وتطبيقها. إن الاستجابة لهذه الحالات سَتزيدُ من التكاليف التشغيلية لإدارات تقنية المعلومات من جهة، وسَتُصَعِّدُ من العقوبات المالية والقانونية لعدم الاستجابة من جهة أخرى.

لقد بدأت المحاكم تأمر بالتعويض في قضايا خطأ بعض الشركات الشائن في مسائل الخصوصية الشخصية، مثل سرقة بطاقة الائتمان لأعداد كبيرة من الأشخاص من قواعد بيانات الشركة المحمية بشكل رديء، وسرقة سجلات طبية من ملفات المستشفى، والسماح بالاستمرار بسرقة هوية زبون رغم قيامه بإعلام المنظمة بحدوث السرقة. يحتاج كبار الإداريين والمدراء التنفيذيين في تقنية المعلومات أن يكونوا واعين لهذه التوقعات والتحديات القانونية، أثناء تخطيطهم الإستراتيجي للاستثمار وللتقنية، لكي تؤخذ هذه التغيرات بعين الاعتبار في الأنظمة والعمليات الموجودة بكلفة أقل منذ البداية، بدلاً من أن تضاف في اللحظة الأخيرة بتكاليف كبيرة.

القسم الأول

قضايا الحوكمة

الموازنة بين سهولة النفاذ والتحكم به

كيف تقرر الإدارة من الذي يسمح له بالنفاذ إلى بعض المعلومات، ومن لا يتوجب عليه النفاذ إلى معلومات أخرى؟ هل يعني السماح لكل الأشخاص بالوصول إلى جميع المعلومات الفقدان الكامل لسيطرة الإدارة؟ كيف يمكن إدارة التحكم بالمعلومات مع تلبية رغبة الزبائن بأن يحصلوا على النفاذ المباشر لمعلوماتهم على مدار 24 ساعة وطوال الأسبوع، من خلال بوابات الإنترنت العامة؟

يستعرض هذا **القسم** عدة مواضيع رئيسية حاسمة تتعلق بآليات الموازنة بين سهولة النفاذ والتحكم به. الموضوع الأول يعالجه **الفصل الثاني** من هذا الكتاب وهو فصل واسع حول التنسيق بين متطلبات الأمن والإجراءات المضادة، وعمليات الشركة، وهي عناصر تتطلب قرارات جوهرية من الإدارة العليا وتوجيهات حيالها باعتبارها تشكل الإطار العام للهيكلية الإدارية لتقنية المعلومات ككل، وللتقنية المشتراة لدعمها.

بعد ذلك، وفي **الفصل الثالث**، تأتي مناقشة مسهبة حول حماية معلومات الزبائن ـ وهي عنصر أساسي في كلّ خطةٍ تتعلق بأمن المعلومات. يركز **الفصل الرابع** وهو فصل رئيسي على المحاور المتعددة لإدارة المخاطر خصوصاً: الأشخاص، والعمليات، والتقنية والتسلسل الهرمي لأجهزة التحكم.

توجد في **نهاية هذا القسم** مناقشات حول تكاليف عائدات برامج أمن تقنية المعلومات، ومدى الاطمئنان إلى الأنظمة الموثَّقة، وأفضل الممارسات في حال مشاركة البيانات خارج المنظمة.

الفصل الثاني

التنسيق بين متطلبات الأمن، والإجراءات المضادة والعمل

كريج اي. كوشر

جامعة الدفاع الوطني، الولايات المتحدة الأمريكية

المقدمة

تُبَيِّنُ، مرةً أخرى، إحصائياتُ نهايةِ السنةِ الأخيرةِ الصادرةُ عن مركزِ التنسيق CERT (CERT-CC) في جامعة Carnegie Mellon، عدمَ وجودِ ما يثبت التحسُّنَ في الاطمئنان على المعلومات. إن مجموعةَ الحوادثِ التي أبلغ عنها لـ (CRET-CC) مجدداً قد وصلت إلى ضعف تلك الخاصة بالسنة السابقة تقريباً، وتجاوزت للمرة الأولى العدد ذا الأرقام الستة 137,529 المسجل عام 2003 (CERT, 2004).

إن المسوحات المتعددة، لمجتمع شركات الأعمال، قد قدَّرت تكلفة انتهاكات أمن المعلومات ببلايين الدولارات. ولقد قدَّر المسحُ الذي أجرتهُ شركةُ الأمن (Trend Micro) تكلفة المخاطر الناتجة من فيروسات الحاسوب وحدها بـ 55 بليون دولار في كل أنحاء العالم في عام 2003 (Reuters, 2004). وقد أوضحت نتائجُ مسحٍ آخر شَمَلَ حكوماتٍ ومدراءَ شركاتٍ من أنحاء العالم، أجرته شركة (Price Waterhouse Coopers & CIO Magazine)، بأن أولى

أولوياتهم في عام 2004 يجب أن تكون رفع وعي المستخدم (CIO, 2003). وهذا يشير إلى أن التشديد على أهمية أمن المعلومات، عبر المنظمات من قمة إدارتها إلى قواعدها، لا يزال ناقصاً.

تستمر المنظمات الحكومية أيضاً بالسعي الحثيث إلى ضمان أمن معلوماتها. ولا تزال الوكالات الحكومية الفيدرالية في الولايات المتحدة الأمريكية تُذكَر كأحد الأمثلة على ضعف حماية المعلومات لديها. فلقد ذَكَرَ تقرير كانون الثاني/يناير لعام 2003 الصادر عن مكتب المحاسبة العامة (General Accounting Office - GAO) أن العديد من الوكالات الحكومية الفيدرالية قد لاحظت «الانتباه المتزايد والشعور بالمسؤولية من قبل إدارتها في مجال أمن المعلومات» وذلك منذ صدور تشريع قانون إصلاح أمن المعلومات الحكومية في عام 2001م، ولكن «على الرغم من تقدم هذه التحسينات إلا أن التحقيقات الحديثة مع أربع وعشرين وكالة، تعتبر من أضخم الوكالات الفيدرالية، أظهرت ضعفاً كبيراً في أمن المعلومات، الأمر الذي يجعل العمليات الفيدرالية الحساسة والأصول في كلٍّ من هذه الوكالات في خطر» (GAO, 2004). يحدد هذا التقرير، على وجه الخصوص، أن إدارة برامج أمن المعلومات والتحكم بالنفاذ هما نقطتا الضعف الأكثر شدة في أغلب الأحيان. في الواقع إن إدارة برنامج أمن المعلومات المُعرَّفة من قبل (GAO) على أنها: «إطار العمل الذي يضمن بأن المخاطر قد فُهِمَت وبأن آليات التحكم الفعّالة قد اختيرت وطُبِّقت كما يجب»، كانت المشكلة الوحيدة التي وجدت ضعيفة في كل وكالة من الوكالات الأربع والعشرين الرئيسية المدققة. إن هذه النتيجة لم تتغير عن نتيجة التحقيق الذي أجرته الـ (GAO) في السنة التي سبقتها.

لماذا تبقى إدارة برنامج أمن المعلومات نقطة الضعف لدى كلِّ وكالةٍ فيدراليةٍ تقريباً؟ ولماذا انعكس هذا الأمر أيضاً على عالم الشركات؟ قد يتساءل المرء كذلك لماذا يبقى نشرُ الوعي الهمَّ الأعلى، بالرغم من هذا الانتشار الواسع والتأثير الكبير للحوادث. ما هي العقبات التي تواجه كلاً من الصناعة والحكومة في إعطاء صفة الهيكلية المؤسساتية لموضوع أمن وتأمين المعلومات في عصر المعلومات؟

عندما يسمع العديد من الأشخاص بمصطلحات تأمين أو أمن المعلومات، فإنهم ينصرفون إلى التفكير في المشكلات. مما لا شك فيه أن ذكر مصطلحات

تأمين أو أمن المعلومات للعديد من الأشخاص اليوم، يذكرهم على الفور بالمشاكل التي عانوها شخصياً، أو عانتها منظماتهم مع آخرِ جولةٍ من جولات البرمجيات الخبيثة، الـ (malware). أحياناً وفي المنظمات التي تتعامل مع معلومات أكثر حساسية أو سرية، يفكر الأشخاص المعنيّون بمشكلتهم الأكبر، ألا وهي التهديد من داخل المنظمة.

قد يقول الأفراد المطلعون تقنياً، وعن قناعة راسخة، أن المشكلة تكمن بشكل رئيسي في انتشار توزيع واستخدام البرمجيات غير الآمنة أصلاً. من جهة أخرى، إن الأشخاص الذين يقرأون الكثير من المنشورات العامة والقصص الإخبارية قد يقولون بأن المشكلة الكبيرة في أمن المعلومات اليوم تكمن في ما هو لاسلكي.

إن لوم ما يسمى بالقراصنة (hackers) شائع جداً، إلا أن هذه الفكرة قد عفّ عليها الزمن. وثَمَّة أشخاصٌ أيضاً يحبون أن يظهروا لنا على أنهم مفكرون إستراتيجيون كبار بكل معنى الكلمة، وعلى أنهم يُمعنون النظرَ في «كراتهم الكريستالية السحرية» ليتنبأوا بالمستقبل، يَدَّعون بأن شكلاً جديداً من الإرهاب، إرهاب الـ (cyber)، يحوم الآن فوقنا وأن هذه المشكلة كبيرة وكبيرة جداً.

إن هذه النظرة إلى تأمين المعلومات نظرةٌ سلبية في أحسن الأحول، وغير مجدية البتة في أسوأ الأحوال. في الواقع قد تكون النقيضَ لحقيقةِ الأمن الفعَّال للمعلومات. لأن حصرَ المشكلةِ في بضعِ مهدداتٍ لأمن معلوماتك وأنظمتك، رغم وجود العديد من هذه المهددات، وكذلك في بضع ثغرات في معلوماتك وأنظمتك، رغم وجود العديد العديد من هذه الثغرات، هو أمرٌ يجعلُ مُعالجتكَ للمسألةِ خارجةً عن السياق الحالي لها، ويتجاهل متطلبات أمن المعلومات، وربما سيؤدي إلى منهجية ترقيعية للحد من المخاطر المستقبلية على معلومات منظمتك.

لذلك إذا نَقَّبنا بعمقٍ أكبر في «المشكلات»، قد نبدأ بطرحِ بعضِ الأسئلة كهذه:

هل فَعَلنا كلَّ ما بوسعنا القيام به من أجل حماية جميع الطرق المحتملة التي من خلالها يمكن أن تُدَسَّ الفيروسات والديدان والبرمجيات الخبيثة الأخرى (malware) داخل بيئتنا؟

ماذا نفعل كي نحدّد ما إذا كان المتقدمُ الجديدُ للوظيفة، أو الموظفُ لدينا من فترة طويلة، يمكن أن يُشكِّل تهديداً داخلياً ماكراً؟ وكذلك ماذا نفعل على الدوام لتسهيل عمل الموظف غير الخبيث؟

هل نحن مُضطرون حقاً إلى جعل منظمتنا جزءاً من اختبار (Beta) العالمي للنسخة الأخيرة من «Server Software X» قبل أن نملك بعض التأمين حول أمنها وثباتها؟

منذ سنوات قليلة مضت، قلق الأشخاص القائمون على أمن المعلومات بشأن المودم الخبيث «Rogue modem» الذي سمح بـ «باب خلفي» أو قناة سرية إلى البنية التحتية للمعلومات. قد تكون المشكلة الآن مع الشبكات اللاسلكية أكبر بكثير، إذ بينما يسمح المودم الخبيث لمستخدم واحد فقط بالنفاذ إلى محطة العمل المحددة تلك، قد تقَدِّمُ نقطة النفاذ اللاسلكي الخبيثة في المكان الخاطئ «باباً خلفياً» أو وصولاً سرياً لعدد غير معلوم من التهديدات المحتملة.

قد نعتقد أيضاً، أن إدارة نظام المعلومات «the sys admins» أو أشخاص الشبكة «the network guys» يقومون بالاهتمام باحتياجات أمن معلوماتنا. ولكن، أليست هذه المهمة تبدو وكأنها قد أتت من مصدر خارجي؟

ومن قد يرغب بمهاجمتي أنا الإنسان المسكين، المتقدم في السن، والجالس هنا على حاسوبي المكتبي، أهتمُّ فقط بشؤوني الخاصة، وأقوم بعملي الذي لا يهدد أيَّ شخص؟

ولكننا إذا ابتعدنا خطوة واحدة عمّا يُدركُ وما يُوصفُ في أكثر الأحيان بـ «مشاكل» تأمين معلوماتنا، نكتشف مجموعة من التصرفات، والوظائف، والمسؤوليات، كما نكتشف مجموعة من الاعتقادات، ولا نعرف من المسؤول عنها جميعها!!، ونكتشف أنها ليست منتشرة في جزء واحد فقط من المنظمة، بل في المنظمة بأكملها.

إننا اليوم في تماسٍّ دائم مع المعلومات وأنظمة المعلومات، في المنزل وفي العمل وفي كل موقع، وفي الطريق بينهما. ربما أصبحنا غير واعين، بأننا على استخدامٍ دائم للمعلومات وتفاعلٍ مستمرٍ مع الأنظمة.

لدينا احتياجات متنوعة، مهنياً وشخصياً وفي سياقات مختلطة، تجعلنا بحاجة إلى الاهتمام بأمن المعلومات. وقد تتغير متطلبات أمن المعلومات هذه عندما ننتقل بين عملنا وحياتنا الشخصية.

تزداد وسائل تأمين المعلومات من حيث الكمية، كما نأمل أنها بازدياد أيضاً من حيث النوعية، ولكن هل تزداد بسرعة كافية؟ وهل ندرك ونوظف بفاعليةٍ جميعَ الوسائل اللازمة لتلبية الحاجات؟

إن المشكلة الحقيقية في أمن المعلومات اليوم، هي أننا قد لا ندرك السياق الكامل الذي توجد فيه المعلومات المتوفرة والمستخدمة من قبل منظمتنا. فمن الممكن أن يكون لدينا نقص في فهم متطلبات أمن المعلومات، ومن المحتمل أننا لا نعلم ما هي الوسائل والوظائف والمسؤوليات اللازمة لتلبية متطلبات أمن المعلومات هذه.

يحتاج المدير التنفيذي أو كبير الإداريين، وعلى كل المستويات في المنظمة، أي مستوى الإدارة العليا والمستوى الاستراتيجي والمستوى التنفيذي، إلى الإلمام بحدٍّ أدنى من الوعي في فهم العلاقة بين هذه الأمور الثلاثة: السياق، والمتطلبات والوسائل. ففهم كل من هذه الأمور بالإضافة إلى فهم العلاقة فيما بينها، يعدّ هاماً لكلٍّ من مسألة أمن المعلومات ومسألة هيكلية المنظمة أو الشركة.

سيركّز هذا الفصل على جمع ثلاثة توجهات بازغة، ألا وهي: «متطلبات أمن المعلومات»، و«هيكلة المؤسسة»، و«الدفاع المعمّق عن المعلومات». وتستطيع هذه التوجهات أن تُشَكِّلَ إطاراً للعمل بأسلوب منسقٍ يَشرحُ متطلبات تأمين المعلومات الخاصة بكلِّ هيكليةٍ إداريةٍ، بالإضافة إلى تحديد طرقٍ فعّالةٍ للحد من المخاطر. من الضروري إقامة العلاقة بين هذه الاتجاهات الثلاثة وفهمها: متطلبات أمن المعلومات، و«هيكلة المؤسسة» وإجراءات «الدفاع المعمّق عن المعلومات».

إن فهم هذه العلاقة سَيُمَكِّنُ المنظمات في كلٍّ من القطاع الخاص والحكومي من زيادة فعالية برامج أمن المعلومات لديها إلى الحد الأعلى.

ماذا نريد؟

إن الخطوةَ الأولى في بناء برنامجٍ فعّالٍ لتأمينِ أو أمنِ المعلومات، هي أن نفهم تماماً ماذا نريد عندما نرغبُ «بالأمن» أو «التأمين». ما هي النتيجة المحددة التي نرغب بإدراكها؟

فكّر في مثالِ بناءِ منزلٍ لك. إن المتطلب الذي يريده كلُّ شخص تقريباً عند بناء منزل، هو أن يكون ذلك المنزل آمناً ومحمياً. هل يكفي أن تقول لمن سيقوم ببنائه: ابنِ لي منزلاً آمناً محمياً، وأن تتوقع بعد ذلك الحصول على ما طلبته تماماً؟ قد تؤوَّلُ عبارة «آمناً ومحمياً» بطرقٍ مختلفةٍ عديدةٍ تبعاً للدور الذي يلعبه الشخص في عملية البناء.

ماذا تعني عبارة «آمن ومحمي» بالنسبة إلى الوالدين اللذين لديهم العديد من الأطفال الصغار؟ هل عبارة «مصمم لمقاومة صدمات الأطفال» ستكون أكثر دقة؟ وعلى الجانب الآخر من سُلَّم العُمر، قد تعني عبارة «آمن ومحمي» للزوجين المتقاعدين الكبيرين في السن تصميماً منزلياً مختلفاً تماماً.

قد تملكُ عبارةُ «آمن ومحمي» بعضَ المعاني المختلفةِ أيضاً تبعاً للبيئة التي سيبنى فيها المنزل. ربما توجد متطلبات بنائية خاصة بسبب تكرار حدوث الأعاصير أو الزوابع أو حتى الزلازل في المنطقة. من الممكن لدرجات الحرارة العالية أو لهطول الثلج الكثير أن تصبح عوامل في تحديد ما تعنيه عبارة «آمن ومحمي» فعلاً.

وبالطبع فإن عبارة «مقاوم للنار» قد تكون أيضاً مثالاً محدداً لعبارة «آمن ومحمي». وأخيراً فإن مالكي المنازل المحتملين قد يهتمون ببساطة بالأمن الفيزيائي أو المكاني.

بالإضافة إلى رغبات **طالبي تملك** المنزل في الحصول على منزل آمن ومحمي، قد توجد أيضاً **أطراف أخرى** لها نفس الاهتمامات بمعنى «آمن ومحمي» أو لها اهتمامات مختلفة. فعادةً ما يطلب مالكو المنزل قرضاً، ولكن كي يحصلوا على هذا القرض، سيتوجب على طرف آخر أن يكون معنياً كذلك، ألا وهو شركة تأمين. سيحتاج مالكو المنزل من أجل الحصول على القرض إلى بوليصة التأمين هذه، ومن أجل الحصول على البوليصة أو كي

يكونوا قادرين على شرائها، سيحتاجون إلى إقناع شركة التأمين بأن المنزل يستحق التأمين. فشركة التأمين لن تقبل منح البوليصة إلى منزل كما يقول المثل «مصنوع من القش»، ستفضل المنزل الذي يبنى بشيء أقوى وأقل قابلية للاحتراق.

قد يتوجب كذلك على كلٍّ من مالك المنزل والبنّاء وآخرين مثل البنك وشركة التأمين، أن ينتبهوا إلى المعايير والقوانين الحكومية فيما يتعلق بالمنازل «الآمنة والمحمية»، مثل القواعد الخاصة بكل منطقة وقوانين البناء. في الحقيقة قد توجد حتى عقوبات وحوافز فيما يتعلق بالالتزام بالمعايير والقوانين مثل: غرامات من قبل البلدية المحلية لعدم التقيد بالقواعد الخاصة بالمنطقة، وأقساط تأمين أقل، تعويضاً على تطبيق متطلبات أمن فوق الحد الأدنى الذي يفرضه القانون. توجد أيضاً في بعض المناطق متطلبات مفروضة من قبل اتحاد مالكي منازل المنطقة نفسها. ومع أن مثل هذه الاتحادات لا تحتاج عادة إلى تطوير معايير وقوانين من أجل الحماية والأمن، إلا أنها تستطيع أن تساهم في فرض إضافات رئيسية كشروط للحصول على رخصة بناء صادرة عن الحكومة المحلية، كما أنها تستطيع أن تساهم أيضاً بالأمن من خلال أنشطة مثل برنامج مراقبة الجوار.

وهكذا فإن لعبارة «آمن ومحمي» معاني مختلفة حسب وجهة النظر المعينة. وقد تكون جميع وجهات النظر المختلفة صحيحة وتقتضي التطبيق. كما يجب على مالك المنزل أن يَفهم جميع هذه الرؤى المختلفة.

إذاً ما هي متطلبات أمن المعلومات؟

لقد سعت المنظمات الحكومية، في محاولتها لتحقيق أمن معلوماتها، إلى جلب جميع المعنيين بهذه المسألة إلى نفس المستوى من فهم متطلبات ذلك. إن العنصر الأول الذي نحتاج إلى فهمه هو متطلباتنا من أجل أمن المعلومات.

لقد أصبحت المفردات الخمس التالية: السِّرية، وسلامة البيانات، والجاهزية، وعدم الإنكار، والتحقق من الهوية أو التوثيق، نوعاً ما القائمة «التقليدية» للمتطلبات. لقد سُجِّلت وحددت في كلٍّ من وزارة الدفاع (DoD) ووثائق الحكومة الفيدرالية الأمريكية مثل: «مسرد ضبط المعلومات الوطني» الذي نشر من قبل «لجنة أنظمة الأمن الوطنية» (CNSS) كتعليمات رقم 4009

(NSTISSC, 2004). ولكن هذه كلها قد لا تتضمن كل متطلبات أمن المعلومات لجميع البيئات ولكل المؤسسات.

لقد حدد المعيار العالمي المسمّى «النموذج المرجعي لهيكلية أمن المعلومات» الصادر عن المنظمة الدولية للمعايير (ISO, 2004) (ISO 7498-2) سبعة مستويات، عاكساً رؤية عالية المستوى لمتطلبات أمن الشبكات الحاسوبية، ومضيفاً بذلك إلى العناصر التقليدية المستويين التاليين: التحكم بالنفاذ، والتوثيق/الإمضاء.

وفي بحث لشركة (Garther Group) يضيف الخبير (روبيرتا ويتي) العديد من المتطلبات إلى المفردات الخمس التقليدية ومنها: التفويض، والخصوصية، وعدم التدخل (Witty, 2002).

ويؤكد كذلك كلّ من غوربريت ديلون وجيمس باك هاوس بعضاً من المتطلبات التقليدية، بينما اقترحوا ثلاثة مبادئ إضافية مختصرة في ما يدعونه (RITE) تشتمل على: المسؤولية، والثقة والأخلاقية (Dhillon, 2000).

قد تتضمنُ القائمةُ متطلباتٍ أكثرَ تبعاً لما وصفه هولميس ميللر بـ «الأبعاد العشرة لجودة المعلومات» وهي: الصلة بالموضوع، والدقة، والتوقيت المناسب، والاكتمال، والترابط، والبنية، وسهولة المنال، والملاءمة، والأمن، والشرعية (Holmes, 1996).

وأخيراً، إضافة إلى العديد من المتطلبات التي عددت حتى الآن، أضاف باحثا شركة IBM (آروون ناغراجان وأنبازهاجن ماني) إلى قائمتهما «المتطلبات الرئيسية لدعم جودة الخدمات» المتطلب التنظيمي (Mani, 2003).

السؤال الآن: أي قائمة من هذه القوائم نتقيّد بها؟ قد يجادل البعض أن بعض المفردات متضمنة أساساً في تعريف مفردات أخرى، فعلى سبيل المثال: عدم الإنكار والتحقق من الهوية هي أجزاء من السِّرية، وقد يجادل آخرون للعودة إلى مجموعة المتطلبات التي اقترحت عام 1991م عندما وصف جون ماكيومبر (John McCumber) السِّرية، والسلامة والجاهزية كصفات مطلوبة لأمن المعلومات في نموذجه الشهير INFOSEC (McCumber, 1991). لكن مثل هذه المناقشات أصبحت بعيدة عن الواقع.

إن السبب المنطقي وراء ضرورة تحديد متطلبات أمن المعلومات بأكبر

قدر ممكن من الدقة، هو إتاحة الفرصة لاحقاً لتطبيق أكثر الوسائل فعالية لتحقيق هذه المتطلبات. إذ قد يقود تعميم المتطلبات، ضمن مجموعة من الخيارات المحصورة أكثر مما ينبغي، إلى نتائج غير محمودة، فالتعميم يزيد من احتمال اعتماد الإجراءات المضادة أو الوسائل غير الصحيحة أو غير الفعّالة لتحقيق الأمن، كما يزيد من احتمال عدم تحقيق مخرجات أمن المعلومات المطلوبة. وقد يجعل هذا التعميم المنظمة جاهلة بالمتطلبات الجديدة والبازغة.

خذ على سبيل المثال متطلب الأمن المتعلق بالخصوصية، لقد سُنَّ في الولايات المتحدة الأمريكية «قانون مسؤولية وقابلية التداول في التأمين الصحي» عام 1996م (HIPAA) بهدف حماية خصوصية صحة المرضى وحماية المعلومات الطبية. ووفقاً لوزارة الصحة والخدمات الإنسانية في الولايات المتحدة الأمريكية «إن هذه القوانين تحمي السجلات الطبية والمعلومات الصحية الشخصية سواء أكانت على الورق، أو في الحواسب، أو منقولة شفهياً». يتضمن (HIPAA) في الحقيقة «قانوناً للخصوصية» يصف حالات محددة حيث يجب أن تُبحث مفردات السِّرية والسلامة والجاهزية. من جهة أخرى هناك العديد من الحالات التي يمكن فيها الإفصاح عن المعلومات الصحيحة (U.S.A Dept. of Health and Human Services 2003). في هذه الحالة على سبيل المثال إن متطلب الخصوصية ليس أضيق من السِّرية، ولكنه يتضمن أيضاً عناصر أخرى من القائمة «التقليدية». إن مجرد اعتبار الخصوصية كمرادف للسرية سيكون أمراً خاطئاً، كما أن تطبيق الإجراءات المضادة لحماية السِّرية فقط من التهديدات سيكون غير كاف لتحقيق متطلب الخصوصية.

إذا كان فهمُ المتطلباتِ الحقيقيةِ لتأمينِ المعلوماتِ هو الخطوة الأولى للوصولِ إلى أمنِ معلوماتٍ فعّالٍ، فإن العقل المنفتح نحو البحث في طبيعة هذا المتطلب هو أمر ضروري. قد تكون التعاريف المعيارية نافعة من أجل الفهم النظري للمتطلبات، ولكن لا يتوجب استخدامها بدون أخذ الأوضاع على أرض الواقع بعين الاعتبار، والتي تستدعي تحقيق متطلبات أمن معلومات محددة. يتوجب على كل منظمة لديها حاجة لأمن معلومات فعّال أن تقرر أولاً ما هو متطلبها الحقيقي، كما ينبغي بعد ذلك أن تتأكد من أن المتطلب مفهوم بشكل جيد في أرجاء المنظمة.

«الدفاع المعمق عن المعلومات» وفي جميع الاتجاهات

توصل العديد من المنظمات إلى إدراكِ أنَّ أمنَ المعلومات ليس مجرد حماية أنظمة تقنيةِ المعلومات بإدخال مقدار أكبر من التقنية، إذ يتضمن الأمنُ أيضاً مسؤوليةً مشتركةً على عاتقِ كلِّ شخصٍ في المنظمة.

لقد عُمّم نهج «الدفاع المعمق عن المعلومات»» لتأمين المعلومات من قبل وزارة الدفاع الأمريكية أولاً. ويتضمن هذا النهجُ تطبيقَ الإجراءاتِ المضادةِ في مجالات: الأشخاص، وطريقة العمل أو الإجراءات التشغيلية، والإجراءات التقنية، وهذا بغية الحد كلياً من مخاطر أمن المعلومات (Joint Chiefs of Staff, 2003). تشمل الإجراءاتُ الخاصة بالأشخاص أموراً مثل: التدريب، وأمن الموظفين. أما الإجراءات التشغيلية فتشمل: الخطط، والسياسات، والإرشادات، وهي كذلك جزء من الإستراتيجية، وتشمل إجراءات التقنية أيضاً أموراً مثل الأنظمة الاحتياطية، وأجهزة كشف الاختراق و«جدران النار».

ومن الممكن جدلاً أن تشتمل هذه التشعيبات الثلاث لنهج «الدفاع المعمق عن المعلومات» على أية وسيلة أخرى لتأمين المعلومات والحد من المخاطر المحدقة بها. كذلك تتضمن كلٌ منها واحدة من العناصر الثانوية لهذه الإجراءات الثلاثة.

لنفكّر، على سبيل المثال، بنظام كشف الاختراق (IDS). عادة ما ينظر إلى نظام (IDS) على أنه تقنية تقوم إما على شبكة أو على حاسوب مضيف. صمِّمت هذه التقنية للكشف عن نشاطات غير عادية أو محظورة على النظام أو الشبكة. إن هذا مشابه لمثال كشف الاختراق لأمن المنزل (IDS) السابق، فعندما يُكتشفُ أي حادث، سيبلّغ شخص لاتخاذ ما يلزم. يتوجب على هذا الشخص، سواء أكان الموضوع منزلاً أو شبكة حاسوبية، أن يتَّبعَ إجراءً معتمداً يتعلق بطريقة القيام بتحقيقات إضافية ثم يرفع تقريراً عن الحادث. فإذا كان المسؤول عن هذه المتابعة مدرباً تدريباً غير جيد، فإنه في أحسن الأحوال قد يحدث اختراق جديد، وفي أسوأ الأحوال قد تحصل كارثة، سواء في المنزل أو على الشبكة، وذلك بالرغم من القدرات الهائلة للتقنية. بطريقة مماثلة قد تؤدي السياسة الواهنة، أو الإجراء المكتوب بشكل سيئ، إلى جعل الفعالية التقنية موضع جدل.

لذا، وكما في تعميم المتطلبات، فإن التصنيف المبسَّط لعناصر نهج «الدفاع المعمق عن المعلومات» أي: التقنية، أو الأشخاص أو العمليات قد يكون غير مناسب. إن قدراً أكبر من التأمل الدقيق في التبعات والعلاقات المتبادلة الضرورية بين عناصر إستراتيجية «الدفاع المعمق عن المعلومات» يُعدُّ مطلوباً بغية توظيف هذا الدفاع أو الإجراءات المضادة بفعالية.

عموماً، قد تملكُ استراتيجية «الدفاع المعمق عن المعلومات» صفةَ «مضاعفة القوة» التي تزيد في تأمين المعلومات نتيجة المشاركة الفعالة لوحداتٍ أكثرَ من وحدات المنظمة، وبالتالي لعدد أكبر من الأشخاص. وعندما يُوظَّف قدر أكبر من الوسائل والإجراءات المضادة، تولّدُ أدوارٌ أكثر من «الدفاع المعمق عن المعلومات»، وإذا ما أديرت بشكل جيد فإنها ستعزز من فاعلية الإستراتيجية.

ثمة قوائم عديدةٌ أخرى للوسائل، يمكن أن تُشكِّل عناصر محددةً إضافيةً تكون جزءاً من إستراتيجية «الدفاع المعمّق عن المعلومات». يتضمن المعيار (ISO 17799) على سبيل المثال ما يلي: الالتزام، وهيكلية الأمن، وتصنيف الأصول والتحكم بها، وذلك ضمن قائمتها المؤلفة من عشرة عناصر (ISO, 2000).

تَصفُ «أنظمةُ أمن الإنترنت» دورةَ حياةِ إدارة الأمن على أنها متمركزةٌ حول ما يلي: سياسة ومعايير وإرشادات، وأنها المؤلفة من خطوات هي: قدِّر، وصمِّم، ووظِّف، وأَدِر، وادعَم، وعلى أن تكون محاطةً بالتعليم المستمر (Internet Security Systems, 2000).

من جانبٍ آخر تَصفُ «أنظمة البيانات الالكترونية» دورةَ حياةِ تأمين المعلومات على أنها مؤلفةٌ من خطواتٍ هي: قدِّر، واحمِ، وتفحَّص، ودرِّب وراقب (EDS, 2000).

بغضِّ النظرِ عن اعتبارنا لهذه الإجراءات على أنها فكرة، أو عملية، أو دورة حياة، أو أنها أيُّ شكلٍ آخر، فإن المهمَّ هو إدراكنا أن هذه الوسائل هي أكثر بكثير من التقنية التي يفكر بها العديد من الأشخاص عندما يسمعون بعبارة أمن المعلومات، ولذلك فإن أمن المعلومات يستدعي توظيفَ عددٍ أكبر من الأشخاص في المنظمة.

مهندس هيكلية أمن المعلومات، أو المعماري

كما رأينا سابقاً، فقد اكتشف مالكو المنازل بأن لديهم مجموعة منوعة من المتطلبات التي تحتاج الدراسةَ من قبلهم ومن قبل آخرين، إذا أردنا تأسيس منزلٍ آمنٍ ومحميٍ. وكما أن تحديد المتطلبات جاء من عدة مصادر، كذلك هي وسائل تحقيقها.

سيتوجب على مالكي المنازل أن يوظفوا عدداً كبيراً من الوسائل من أجل حماية أنفسهم وأطفالهم، وحماية البنية المادية للمنزل، والبيئة التي سيبنى فيها، وكذلك أمن أموالهم. تشتمل بعضُ هذه الوسائل على منتجات متفق عليها، وعلى ممارسات مثلى، وكذلك على تصاميم وهياكل مراقبة بدقة. ستتضمن وسائلُ أخرى سياسةً مطبقةً ومفهومةً جيداً، وخدمات مراقبة. وبينما تجري عمليةُ بناءِ المنزلِ، سيكونُ كلاً من النجارين والسماكرة والمتخصصين بالكهرباء والمشتغلين بالسقوف، ومزوديهم، والمشرفين عليهم منهكين بالعمل. ستقوم مجموعةٌ من المراقبين بالتأكُّدِ من تطبيق قوانين البناء والخطط الموضوعة. كما سيجري اختبارُ أجهزة البيت، وقبل أن يسكن أخيراً سيمنح وثيقة نهائية.

إذاً من الذي سيكفل أن جميع المتطلبات قد أخذت بعين الاعتبار، وأن جميع الوسائل قد وُظِّفت بفاعلية، وأن كلَّ شيء منسجمٌ ويعمل معاً؟ يجب أن تلتقي متطلباتنا في سياق مشترك مع الوسائل المختارة لتنفيذها و يدعى هذا السياق بـ «الهندسة المعمارية».

سيبتدعُ المهندسُ المعماري مجموعةً من الوثائق التي تُصوِّر المنزلَ من أكثر من منظورة. سيستخدمُ كلُّ واحدٍ من ذوي المهارات المختلفة، الذين سيقومون بإنجاز كلٍّ من الإجراءات أو «الوسائل»، جزءاً من هذه الوثائق المصممة من قبل المعماري تجعلُ إنجازهم مُتَّسقاً مع السياق الإجمالي للمنزل. إن الوثائق المخصصة للنجارين على سبيل المثال: سَتَعرِض محاورَ البناء المتعلقة بالنجارة فقط.

سيكون المهندسُ المعماري هو المتحكِّم المركزيّ بجميعِ هذه الوثائق والرسوم المنظورية. وإذا كان لابد من إجراء تعديلات في واحد من الأنظمة، على سبيل المثال: شبكة الأسلاك الكهربائية، فإن المهندسَ سيتأكدُ من أن هذا التغييرِ لا يؤثر سلبياً في أيِّ محورٍ آخر للمنزل.

لن يخدم التوثيق الهندسي الجيد الهدف منه أثناء بناء المنزل فقط، بل

أيضاً بعد الانتهاء من عملية البناء. فإذا استطاع مالكو المنازل الاحتفاظ بمجموعةِ الرسومِ الهندسية، فسيتمكنون بعدها من العودة إليها طيلة فترة ملكيتهم للمنزل، وكلما رغبوا بإجراء تعديل له. قد يختار مالكو المنازل أن يضيفوا ملاحظاتهم على الوثائق الهندسية أو أن يوائموها كي يمتلكوا رسماً دقيقاً وحالياً لعلاقات المقومات المختلقة للمنزل.

هيكلة أو عمارة المؤسسة

نشوء فرصة

إن «تأمينَ المعلومات» و«هيكلةَ المؤسسة» ليست أفكاراً أو برامجَ جديدةٍ. في الحقيقة، إنهما في الحكومة الفيدرالية الأمريكية مثلاً، نشاطان رسميان يُحدَّدُ لكلٍّ منهما متطلبات ورفع تقارير وفق سياسات وقوانين وقواعد موضوعة. من جهة أخرى فإن برامجَ «تأمين المعلومات» يغدو نشاطاً رسمياً أيضاً في المؤسسات من خلال القوانين مثل قانون (HIPAA) في قطاع الخدمات الصحية، وقانون (Sarbanes-oxley) لشركات التدقيق والمحاسبة العامة، وقانون (Gramm-leacch-Bliley) لشركات الخدمات المالية. إلا أنه لا توجد بعد أوامرُ رسمية تنظيمية أو قانونية لـ «هيكلة المؤسسة» في القطاع الخاص، إلا أن العديدَ من الشركات تختار أن تتبنى شكلاً منه كأفضل الممارسات.

لماذا تُستخدم «هيكلة المؤسسة» في الحكومة؟ تُسأل الوكالات الفيدرالية الأمريكية مثلاً عن تعليل إنفاقها على تقنية المعلومات وعن بيان كيف تَدعمُ أنظمةٌ لديها إنجازَ مهمتها. تتضمن جهودُ «هيكلة المؤسسة» أكثرَ من مجردِ خبراء لتقنيات المعلومات للمنظمة. في الواقع تتضمن الخطوات الحكومية الأولية المتخذة لتحديد «هيكلة المؤسسة» الفيدرالية وضعَ نموذجٍ مرجعي تجاري على أن تتبعه فيما بعد نماذج مرجعية تقنية ومعلوماتية.

تُقدِّمُ برامجُ «هيكلة المؤسسة»، في كلٍّ من الوكالات المدينة للحكومة الفيدرالية ووزارة الدفاع الأمريكية، مجموعة من: النظرة المستقبلية، وترابط العمل، والرؤى التقنية والتشغيلية للمهمة أو العملية. فمثلما يقدم مهندس المنزل المعماري لكلٍّ مختصٍ الرسمَ المنظوري الخاص به، فإن مهندسي الحكومة المعماريين يقدمون مجموعةً من الرؤى المترابطة والمراقبة المركزية. وبالتالي يستطيع المدراءُ التشغيليون أن يروا الرسم المنظوري

المتعلق بطريقة العمل، بينما يرى مختصو تقنية المعلومات الرؤى التقنية.

لقد وُجد في الماضي تنويه أو دمج بسيط جداً «لتأمين المعلومات» داخل «هيكلة المؤسسة» وهذا حتى في الحكومة الفيدرالية الأمريكية حيث كلا البرنامجين نشاطان رسميان. بدأ هذا بالتغيير بسبب انتشار الوعي بأهمية «تأمين المعلومات» وقد بدأت التنويهات إلى عناصر تأمين المعلومات بالظهور في النسخ الأخيرة لأطر العمل في «هيكلة المؤسسة» الفيدرالية.

سواء جرى اعتمادُ نهج مثل «إطار عمل هيكلة المؤسسة الفيدرالي» (FEAF)، أو مثل «إطار عملٍ هيكلية المؤسسة لوزارة الدفاع» (DOD) أو أيِّ نهج آخر تتبناه المنظمة وترعاه، فإن ذلك لا يهم شريطة أن يتضمن نظرةً شموليةً تحتوي العناصر التجارية والتشغيلية والتقنية.

وقد يَقترحُ البعضُ أيضاً اعتمادَ نهج زاشمان أو تعديلاً عليه، وعلى الرغم من أن كلا هذين الاتجاهين وُلِدا من العمل في هيكلية تقنية المعلومات، إلا أنهما محدودان عند محاولة استعمالهما لوصف السياق الشمولي لأمن المعلومات (Zachman, 2001).

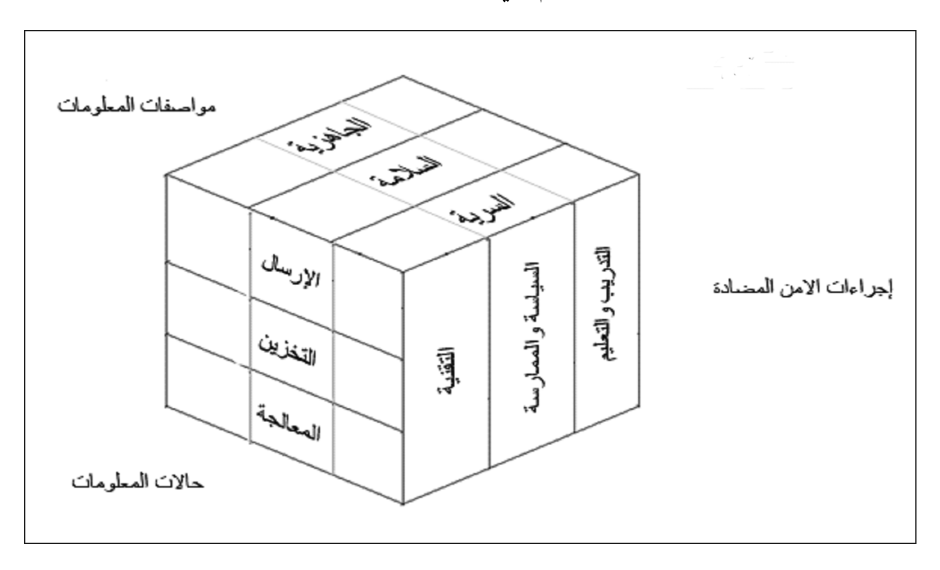
إن الاتجاه الشمولي هو الاتجاه المفضل، لأننا نريد لسياقنا أن يكون مركزاً على المعلومات وليس على أنظمة المعلومات أو على تقنية المعلومات فقط؛ إذ نريد بالنتيجة أن نحدد متطلباتنا لتأمين المعلومات وليس لتأمين نظمها أو تقنيتها. فنحن نحاول تجنب فقدان المعلومات وليس تجنب فقدان النظام أو التقنية، وهي مشكلة مختلفة تماماً (Von Solms, 2001).

إلتقاء المتطلبات والوسائل والهيكليات

عند عملنا على فهم متطلبات تأمين المعلومات، يجب أن نهتم أيضاً بالوسائل أو «الإجراءات المضادة» لتنفيذ هذه المتطلبات، وأيضاً السياق أو الهيكلية التي تتوافق معها، فإن فهمَ ارتباط هذه الأشياء الثلاثة لأمرٌ مهمٌ. قد يبدو أن استيعاب مثل هذه المجموعة المعقدة من العلاقات مهمةٌ مروعةٌ. لحسن الحظ، ثمَّة مجموعةٌ من النماذج التي تساعد على شرح ارتباط المتطلبات، والوسائل، مع الهيكليات.

في عام 1991م اقترح جون ماكيومبر (John McCumber) ما دعاه «النموذج

الشامل» لأمن المعلومات المرسوم في الشكل (1) (McCumber, 1991).



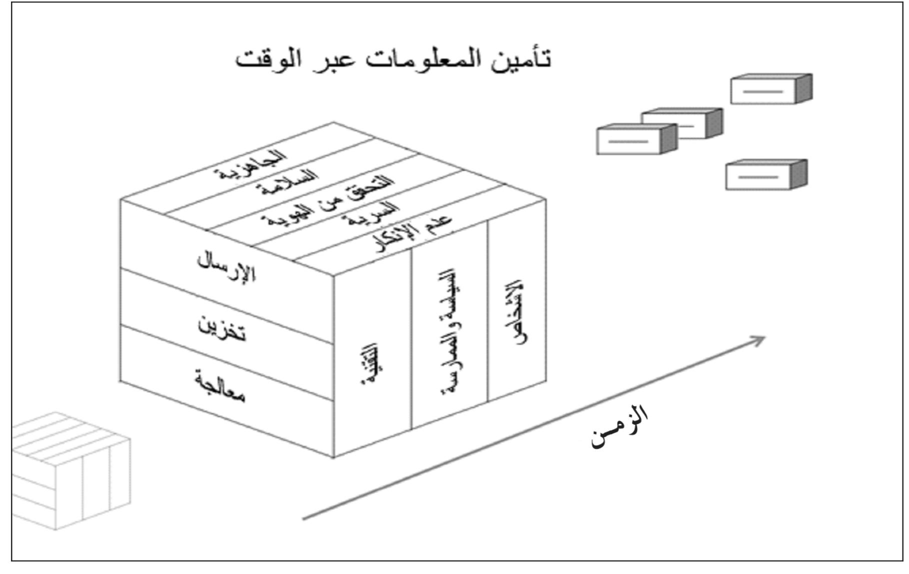
الشكل (1).

إن ما دعوناه بمتطلبات تأمين أو أمن المعلومات، أشير إليها من قبل (McCumber) بـ «مواصفات المعلومات». لقد أشار منها (McCumber) إلى: السِّريّة، والتوفر والسلامة فقط.

إنّ ما نسميه اليوم بـ «الدفاع المعمّق عن المعلومات» سمّاه (McCumber) إجراءات الأمن المضادة. فلقد حلَّت كلٌّ من الأشخاص، والعمليات والتقنيات في «الدفاع المعمق عن المعلومات» محل مقومات (McCumber) الثلاثة في إجراءات الأمن المضادة أي: التقنية، والسياسة والممارسة، والتدريب والتعليم. أما الجانب الثالث لنموذج (McCumber) أي ما سمّاه بحالات المعلومات، فقد قال (McCumber) أن جميع المعلومات توجد في حالة من هذه الحالات الثلاث: الإرسال، أو المعالجة، أو التخزين. وقد أجاز (McCumber) أن توجد المعلومات أحياناً في حالتين من الحالات الثلاث في نفس الوقت. في نظام الرسائل على سبيل المثال، تستطيع الرسالة حينما تكون في حالة الإرسال أن تكون في حالة التخزين أيضاً.

وعلى صعيد آخر، وصف (Maconachy [et al.], 2001) في عام 2001 كيف تطور نموذج (INFOSEC) إلى نموذج تأمين المعلومات (IA). إن هذا التطور

هو أكثر من مجرد تغير دلالي بسيط أو تغيير أسماء. اقترح مؤلفو هذا النموذج الجديد عدداً من التغييرات لتحديث نموذج (McCumber). فالعناصر التي أَطلقَ عليها (McCumber) اسمَ «مواصفات المعلومات»، أشير إلها من قبل هؤلاء المؤلفين بـ «خدمات الأمن» وقد وُسِّعت لتتضمن التَّحقق من الهوية وعدم الإنكار. لقد قام نموذج 2001م بتحديث إجراءات الأمن المضادة (McCumber) إلى ثلاثية «الدفاع المعمق عن المعلومات» الحالية، ألا وهي الأشخاص، والعمليات والتقنية. أما الجانب الثالث لنموذج (McCumber) أي «حالات المعلومات»، فقد تُرك بدون تغيير. اقترحَ المؤلفون بأن بُعداً رابعاً، ألا وهو الوقت أو الزمن، يجب أن يؤخذ كذلك بعين الاعتبار بطرق عديدة. رسم نموذج 2001 في الشكل (2) متضمناً الوقت.



الشكل (2).

مع ظهور أطر عمل شاملة لـ «هيكلة المؤسسة» اليوم، تحظى المنظمات بفرصةِ الاستفادةِ من الاتجاهِ الشموليِّ في «هيكلة المؤسسة»، لتحقيق تكاملٍ أكثرَ تقدماً من أي وقت مضى بين متطلبات أمن المعلومات، والإجراءات المضادة، والطريقة التي تُستخدم فيها المعلومات في المنظمة. ويمكن أن يُعدَّ هذا التطور تقدماً في التصور لنسخة 2001 من نموذج (McCumber).

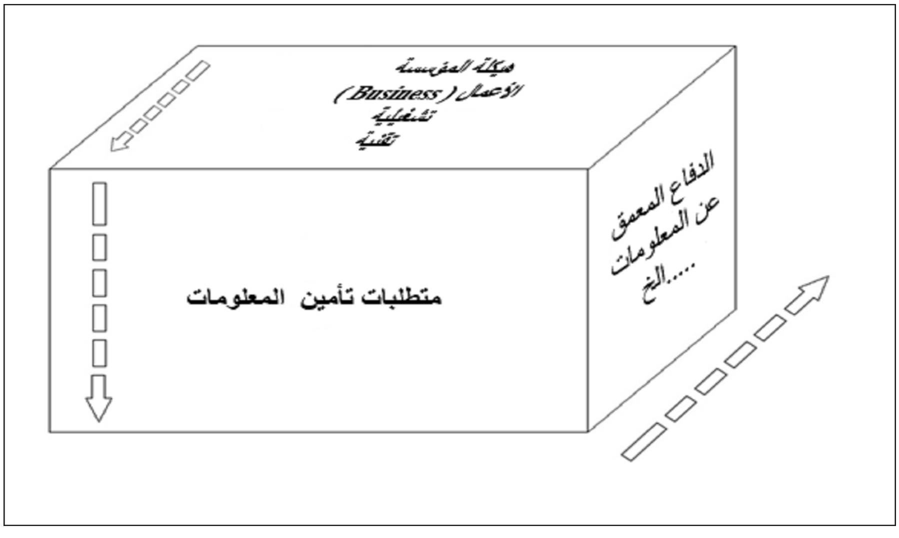
بينما زادت نسخة (Maconachy [et al.], 2001) مواصفات المعلومات الثلاث

لـ (McCumber) إلى خمسِ حالاتٍ أمنية، وحدَّثت إجراءاته المضادة لتعكس المنهج الحالي لـ «الدفاع المعمق عن المعلومات»، بقيت حالات المعلومات الثلاث: الإرسال، والمعالجة والتخزين بلا تغيير.

قد ينظر إلى غاية (McCumber) في وصف «حالات المعلومات»، على أنها طريقةٌ للنظرِ في علاقة المعلومات، عند لحظة معيّنة من الزمن، داخل نظام للحماية والإجراءات المضادة. لقد أثبت نموذجه المفاهيمي على أنه مفيد للغاية في تعليم العاملين في حقل أمن المعلومات. لابد من القول إنه عندما طُرِحَ نموذجُ (McCumber) كانت شبكات حاسوب وأنظمة المعلومات لا تزال في مرحلة الطفولة، وكان نهجُ «هيكلة المؤسسة» لا يزال حلماً بعيد المنال، وبالتالي فإن «حالات المعلومات» لـ (McCumber) مقاربةٌ «جيدةٌ» لوصف هذا البعد الثالث للمكعب.

إن «هيكلةَ المؤسسة» كبديل لـ «حالات معلومات» (McCumber) تسمحُ بمستوى لم يسبق له مثيل من الأمانة والفهم لمتطلبات تأمين المعلومات والإجراءات المضادة وعلاقتهما بكيفية استخدام المعلومات في المنظمة.

يمنحُ استخدامُ «هيكلة المؤسسة» كبعدٍ ثالثٍ المنظمةَ القدرةَ على تفحُّصِ متطلبات تأمين المعلومات بأسلوبٍ منسق ومتكاملٍ من حيث: عمليات المؤسسة، والإجراءات التشغيلية والبنية التحتية التقنية. إن هذا التطوير لنموذج (McCumber) والتحديث من قبل (Maconachy, [et al.]) مبيّن في الشكل (3).



الشكل (3).

ثمة عدد من الفوائد التي تُكتسبُ نتيجةً لهذا الاتجاه الجديد. إذ يؤدي استخدامُ «هيكلة المؤسسة» إلى وجود رابطةٍ بين مهمة المنظمة والتقنية يمكن أن نُطبِّقَ عليها متطلبات تأمين المعلومات والإجراءات المضادة. تُقَدِّمُ «هيكلةُ المؤسسة» كذلك مقاربةً مبنيةً على المعلومات مقارنة بالمقاربةِ السابقةِ التي كانت مبنيةً على النُظمِ أو المنظومات.

باعتبار أن جميعَ عمليات «هيكلة المؤسسة» تنطلقُ من المهمة الرسمية للمنظمة، فإن هذا النموذج الجديد يتضمن حكماً انغماسَ أو مشاركةَ قادةٍ رفيعي المستوى ممّن يقومون بتحديد مهمةِ المنظمة.

عندما تُطبق دقة «هيكلة المؤسسة» بدلاً من حالات المشروع السابقة على البعد الثالث للنموذج، فإن المعلومات تُؤخَذُ في سياق أكثر صلة.

تُوجد «هيكلةُ المؤسسة»، عندما ينظر إليها في علاقتها مع متطلبات تأمين المعلومات والإجراءات المضادة، رؤيةً واضحةً قائمةً على منظورٍ مَبنيٍّ على دور «المتطلبات» و«الدفاع المعمق عن المعلومات». فعندما يَنظرُ أيُّ شخصٍ في الهيكلية التي اعتمدها هؤلاء القادة رفيعو المستوى، سواء كانت هيكلية سيرورة الأعمال، أو العمليات أو التقنية، سيرى بوضوح ما يقابل كلاًّ منها من متطلبات تأمين المعلومات والإجراءات المضادة.

بهذه الطريقة، يُعطى القادةُ رفيعو المستوى أيضاً الفرصةَ ليقروا على مستوى المؤسسة، أيّاً من متطلبات تأمين المعلومات هو الأنسب لكلٍّ من وحدات المنظمة. يجب أن يُمنحَ جميعُ أفراد المنظمة الفرصةَ ليشاركوا في تحديدِ متطلبات تأمين المعلومات والإجراءات المضادة الضرورية التي تخصّ الجهة التي يعملون بها ضمن «هيكلة المؤسسة». يجب أن يمتلك أيضاً كلُّ شخصٍ في المنظمة الفهمَ المناسبَ لسياق دَورهِ في تأمين المعلومات.

استنتاجات

على الرغم من التطورات السريعة في التقنية والسياسات المبتكرة والمقاربات الإجرائية، وبالرغم من التأكيد المتزايد أبداً على التعليم، والتدريب والتوعية، إلا أن تأمين المعلومات لم يُصبح أسهل تنفيذاً. هناك حاجةٌ إلى مقاربةٍ منهجية جديدة تأخذ بعين الاعتبار متطلبات تأمين المعلومات بدقة أكبر،

وتكون شاملةً جميع وسائل الدفاع الممكنة، وتعترفُ بأن المهمَّ في دعم سيرورة أعمال المنظمة هو المعلومات ليس الأنظمة.

إن الجيل الثالث لنموذج (McCumber)، بعد إضافة «هيكلة المؤسسة» له، هو نموذجٌ مفاهيميٌ بامتيازٍ ويُشكِّل قاعدةً لمقاربةٍ تحليليةٍ وهندسيةٍ لتلاقي وتلاؤم المتطلبات والإجراءات المضادة مع المعلومات. إذ يَدمُجُ هذا الاتجاهُ أنظمةَ تأمين المعلومات مع الإدارةِ أكثر من أي وقتٍ مضى، ويُشكِّلُ إطارَ عملٍ يُطَوَّرُ باستمرار.

بما أن التقنية، وسيرورة الأعمال، والتهديدات الموجهة إليهما، تتغير باستمرار، يتوجب على أمن المعلومات أن لا تحاول فقط الاحتفاظ بوضعها وإنما أن تبحث عن الفرص التي تجعلها سَبَّاقَة وأن تبقى في المقدمة. لقد أصبحت هذه العبارة «ضعها كجزء ثابت في البنية ولا تقم بإضافتها لاحقاً» الوصفة الطبية المثلى لمختصي أمن المعلومات لسنوات عديدة. ولكن بناء المنزل الجيد لا يبدأ باجتماع جميع التجار في موقع البناء. إن البناء الجيد يبدأ بخطة. هذه الخطة هي التصميم المعماري. وهذه هي النقطة التي يجب أن تبدأ منها عملية أمن المعلومات أيضاً.

مراقبة الموظف مقابل خصوصيته

إن المنظمات الحكومية والتجارية قادرةٌ في معظم الحالات على مراقبة استخدام الموظف لأجهزتها وشبكاتها المعمارية الممتلكة من قبلها. يكفي لذلك إصدار وثيقةِ سياسةِ العملِ الرسميةِ وتوزيعها على الموظفين كتوجيهات، مُصرِّحةً بأنَّ المنظمة تسمح (أو لا تسمح) باستخداماتٍ محددةٍ للتجهيزات. ويُرافق هذه الوثيقة التصريح بأنه لا يتوجب على الموظف أن يتوقع أَيَّةَ خصوصيةٍ في استخدامه للنظام، هذا كل ما يلزم من أجل تنفيذ السياسة.

ولكن أين يجب رسم الخط الذي يُحَدِّدُ الاستخدامَ الشخصيَّ المقبول؟ إذا ما استثنينا منع النفاذ إلى اللائحة الواضحةَ لمواقع: المقامرةِ، والإباحيةِ، والمستحضراتِ الصيدلية غير الشرعية، ومواقع التواصل الاجتماعية، فما هو المقبول عدا هذا الاستثناء؟ هل يعتبر منطقياً أن يُسمح للموظفين تفحُّص الصفحة الالكترونية للطقس (weather.com) في أشهر الشتاء ليحددوا إلى أي مدى ستكون قوة العاصفة وشيكة الحدوث؟ ماذا عن السماح للوالدين بزيارة

الصفحة الالكترونية لتقديم الرعاية للأطفال والمزودة بكاميرات ليتأكدوا من سلامة أطفالهم؟ ماذا عن تفحص موقع (CNN.com) للأخبار عندما يقع حادث أو كارثة خطيرة بالقرب من المنزل، والتي قد تؤذيهم أو تؤذي أسرهم عند عودتهم إلى المنزل؟

يبدو أن القرار الإداري الذي يعتمد على «العرف العام» في ما هو مقبول وغير مقبول هو أفضل طريقة للحل باعتبار أنه من المستحيل تحديد كل الحالات الممكنة. إن ما هو مهم، من وجهةِ نظرِ كلٍّ من الموظفِ وربِّ العملِ، هو وجودُ خطَّةِ عملٍ مكتوبةٍ تحتوي على توجيهاتٍ تُرسلُ لجميعِ الموظفينَ حتى يكونوا على درايةٍ بها. باعتبار أن التقنية تتقدم باستمرار وباعتبار أن خدمات ومنتجات ذكية جديدة تدخل في الاستخدام، هل على الإدارة الأخذ ببعض الاستثناءات؟ بالطبع ـ إن كلاًّ من وسائل المراسلة الفورية (IM) والهواتف النقالة المزودة بآلة تصوير هما الآن حالتا قلق لمسألة الخصوصية وأمن المعلومات. يجب أن تُطوَّرَ السياساتُ (أو تُوسَّع) للتعامل مع هاتين التقنيتين بحيث تعكس توقعات الإدارة لاستخدامهما (أو عدم استخدامهما) في مكان العمل.

تُراقبُ العديدُ من المنظمات، التي تُوظِّفُ عاملين لخدمة الزبون، مكالمات الهاتف والبريدَ الالكترونيَّ وتُسجلها لتتأكد من خدمة الزبون المتينة وجودَةِ الإيصال. يجب أن يَعلم الموظفون المشتغلون في هذه الأنشطة سياسات ومعايير المؤسسة حول تسجيل محادثاتهم ورسائلهم من خلال تعليماتٍ مكتوبةٍ وأيضاً من قبل المشرفين عليهم. إذا ما نظرنا إلى الموضوع من زاوية أمن المعلومات، نجد أن إعطاءَ الزبائنِ معلومات كثيرةً جداً قد يكون سيئاً كإعطائهم معلومات قليلةً جداً. على سبيل المثال، في حالة التأمين الطبي أو النتائج المخبرية الطبية الروتينية.

في بعض الحالات ـ مثل أسواق الأوراق المالية ووكالات القوات المسلحة والشرطة ـ قد يكون منطقياً إنشاءُ ملف تسجيل الأحداث ومتابعته من أجل تسجيل كل التعاملات التي تحدث عندما يَدخلُ الموظف إلى النظام أو الشبكة، أو يَنفُذُ إلى المعلومات أو يُرسِلُ ملفات. من الواضح أن إمكانية المتابعة هذه غالية الإنشاء والمتابعة، ولكن عندما يحدث أي انتهاك للأمن، تُزوِّدُ هذه المقدرةُ معلومات مفيدة في فهم ما حدث، متى حدث وَمِنْ قِبَلِ مَنْ.

إن جميع هذه التفاصيل حاسمة في تحديد خطورة الانتهاك الأمني الذي حصل، والضررِ المرافقِ له، وما الذي يتوجب فعلهُ للحد من أيّ أثر آخر في المنظمة وأشخاصها وزبائنها ومساهميها.

سياسات إدارة نظام أمن المعلومات

تُطَّبقُ سياساتُ إدارةِ أمنِ المعلوماتِ على نشاطاتِ إدارةِ النظام مثل إدخال أسماء المستخدمين وامتيازاتهم الأمنية. يقومُ بهذه النشاطات عادةً فريقٌ صغيرٌ من مهندسي الأمن أو مهندسي النظام من ذوي الخبرة والموثوقين بدرجة عالية، الذين مُنحوا حَقَّ الوصول إلى حسابات إدارة النظام وكلمات سِرِّه. يلتزم هؤلاء المهندسون باتباع طرائق وسياسات مفصلّة لإضافة أشخاص، وحذف آخرين وتغيير مستويات وصولهم إلى المعلومات. تُقدِّم هذه الطرائقُ تماسكاً، ورقابةً لكلٍّ من الإدارةِ والمستخدمِ في حالة حدوث الأعطال الفنية أو اختراقات الحماية.

يوجد، من وجهة نظر إدارة تقنية المعلومات، عنصران حاسمان للتحكم هما: (أ) وجودُ مدراء موثوقين يتمتعون بخبرة تقنية عالية، (ب) وضعُ سياساتٍ شاملة لإدارة أمن المعلوماتِ تتفق مع احتياجاتِ المؤسسة. يُركِّزُ العديدُ من المنظمات على العنصرِ الأولِ ويفترضُ أن مدير النظام سيُعنى بالعنصر الثاني. قد يكون هذا مقبولاً في بعض الحالات، ولكنه في العديد من الحالات الأخرى لا يكون مدراءُ النظامِ مدربين على رسم سياسةِ أمن معلوماتٍ تتفق مع، وتبقى متبعةً، لأهدافِ عملِ المنظمة.

بما أن أغلبية مشاكل أمن المعلومات هي مشاكل من داخل المنظمة، لذلك ينبغي أن تراجع الإدارة إجراءات وسياسات إدارة النظام على الأقل مرة واحدة في السنة من أجل التأكد من أن مستويات الأمن المطلوبة متّبعةٌ. وإن التعاقدَ على رقابة إدارة النظام من جهة ثالثة والحصولَ على شهادتها تُعدُّ وجهةَ نظرٍ صائبة أيضاً. إن البنودَ المحددةَ التي يجب الأخذ بها في سياسات إدارة أمن المعلومات تتضمن ما يلي:

1. تحديد عدة مستويات للموافقة على إضافة أشخاص جدد إلى النظام (يمنعُ هذا الإجراء وجودَ موضعٍ واحدٍ للفشل).

2. التفقد الدوري لمستويات وامتيازات دخول النظام أمنياً بغية منحِ مستويات أعلى أو أدنى لدخول المستخدم.

3. المبادلة الدورية فيما بين أعضاء الطاقم المسؤول عن منح التراخيص الأمنية وتكليفهم بمهمات مختلفة وجديدة كلّ بضعة أشهر لتقليل فرصة اختراق الأمن الناتجة من اطمئنان الموظف إلى أنه لن يكتشف بسبب بقائه في منصبه لمدة طويلة.

4. ضرورة وجود عملية رسمية لإدارة الوثائق التي تُفَصِّلُ متى أُضيفَ مستخدمون إلى النظام، ومتى حَدَثَت تغييرات في مستوى دخولهم، وفتحُ ملفٍّ خاصٍ بذلك.

5. وجود وظيفة للرقابة وتفتيش أمن المعلومات من أجل تَفقُّد الوثائق والإلتزام بالتعليمات.

6. تَجنُّبُ «تضارب المصالح» المعروفة بين إدارة أمن للمعلومات والمستخدمين، مثل سماح الزوج لزوجته الموظفة معه بدخول مستوى أمني أعلى. ومن المفيد وجود جهة ثالثة حيادية تؤدي عمل إدارة النظام ممّا يحدّ من تسرب مسألة «تضارب المصالح» إلى النظام.

7. التأكُّدُ من أن إدارةَ أمنِ النظام تتلقى تدريباً على جميع محاور التقنية الجديدة التي تعينهم وعلى إجراءات وسياسات المنظمة.

8. ربطُ سياساتِ الأمنِ بالسياسات التي تحمي سيرورة عمل المؤسسة من الهجمات الداخلية والخارجية، ولكنها في نفس الوقت تعمل على تعظيم وصول المزود والزبون إلى المعلومات التي يحتاجونها ليشتروا المنتجات والخدمات أو ليستكملوا مخزون المستودعات.

المساءلة الاحترافية

تواصل أصحاب العلاقات خلال الأزمات وخارجها

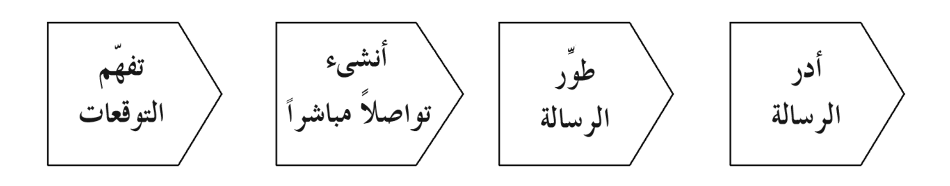
لدى كلِّ منظمةٍ مساهمون أو أصحابُ مصلحةٍ منهمكون في، أو لديهم مصلحة في، عملياتها وإجراءاتها، ونتائجها المالية، أو المواجهةِ مع المواطنين في حالة المنظمات الحكومية. باعتبار أن تقنية المعلومات تُستخدمُ تقريباً في كلِّ شركة، فإن المساهمين على دراية بفوائدها ومخاطرها ويرغبون بتتبع الأخبار الجيدة والسيئة. عندما تسير العمليات على ما يرام مع مشاكل قليلة وعادية، تَصدرُ التقارير الروتينية ويُرسلُ البريد الإلكتروني بآخر الأحداث والأنباء كل

أسبوع أو أسبوعين، ويُعدّ هذا مقبولاً. أما إذا ما حدث أي اختراق لأمن المعلومات مسبباً تعرضاً تنظيمياً أو قانونياً أو مالياً، فإن المساهمين يحتاجون إلى مستوى عال جداً من الاتصالات مع المسؤولين والإدارة العليا. تحتاج إدارة تقنية المعلومات إلى تأسيس أربعة أبعاد للاتصالات:

1. تحديد توقعات الزبون والمساهم.
2. إنشاء قنوات اتصالٍ مباشر.
3. تطوير الرسالة.
4. إدارة الرسالة.

إن لدى مدراء تقنية المعلومات التنفيذيين ولدى الإدارة العليا المشكلةَ نَفسَها التي يعانيها رجالُ السياسةِ المنتخبون وهي: تجاوز «الضجيج الإعلامي»، للإجابة عن الأسئلة، وتقديم المعلومات. في البيئة الحالية للدورة الإخبارية النشطة على مدار 24 ساعة، قد يَقلِبُ أيُّ شيء يحدثُ في العالمِ الأخبارَ الجيدةَ إلى مثبطةٍ للهمَّةِ، والأخبارَ السيئةَ إلى مثيرةٍ. إنها حقيقة من حقائق الحياة اليوم أن يَجمَعَ الزبائنُ والمساهمون المعلومات طوال الـ 24 ساعة وعلى مدار الأسبوع، ويقارنوا المعلومات التي تزودها وسائل الإعلام بتقارير الإدارة، ليدركوا الفروقات إن وجدت. خلال أوقات الأزمة ـ مثل: اختراقُ أمنٍ هام، أو تَسَرُبٌ عَرَضي لملفاتِ أو معلوماتِ الزبون، أو فقدانُ البياناتِ أثناء عاصفةٍ، أو عدمُ القدرةِ على معالجةِ مقاديرَ كبيرة من بيانات المبيعات ـ تُعَرقِلُ كميةُ المعلوماتِ الكبيرةِ «إدراكَ» ما يحصل أو ما حصل بالضبط. ولكن حتى تكسب المؤسسة أو الشركة الدعم السياسي أو دعم المساهم (الذي غالباً ما يكون صعباً جداً) يجب أن يكون هناك تفسيرات بسيطة للمشاكل المعقدة.

نبيّن فيما يلي منهجيةً متعددةَ الأبعادِ من أجل ربط معلومات المساهمِ بكلٍّ من المعلومات السلبية والإيجابية.



البعد الأول:

- حدد توقعات المساهمِ والزبونِ بصدق.
- أدرك «لماذا» (لماذا يهتمون بهذا الوضع؟)
- حدد «متى» (ما توقيت الحدث الذي أثار اهتمامهم؟)
- تعرَّف «من» (من هو الذي يهتم بالضبط؟)
- تفقَّد «كيف» (كيف يستجيبون أو يتفاعلون؟)
- تحرَّ جداول الأعمال السِّرية (لماذا يستاء بعض الأشخاص من دون غيرهم؟).
- سد الثغرة بين المساهم والزبون (ضع نفسك مكان كلٍّ منهما).

قم بطرح الأسئلة لتستخرج منها الإجابات، إذا كانت المعلومات غير معطاة بشكل تلقائي أو غير متوفرة بسهولة. استمع إلى من يتكلم وافهم سبب استماع الآخرين إليه. حدّد مَنِ المستفيد الأكبر، ومَنِ الأقل ربحاً. أكِّد افتراضاتكَ بالتداولِ مع جميع المعنيين لأن التفاصيل قد لا تكون واضحة.

البعد الثاني:

إنشاء قنوات تواصل مباشرة:

لماذا هذا الإنشاء مهم؟ إنه مهمٌ لتجنبِ تسريبٍ أو سوء إيصالِ رسالتك للآخرين الذين قد لا يملكونَ جميعَ المعلوماتِ التي تملِكُها أنت. يَخلِقُ الاتصالُ المباشر «صوتاً» واحداً يخفف من التشويش الذي يحصل نتيجة العديد من وجهات النظر لكلٍّ منَ الأخبارِ السيئةِ والجيدة.

كيف يمكن لهذا التواصل أن ينشأ؟

- أنشر «رسالةً إخباريةً» شهريةً لأمن تقنيةِ المعلومات.
- أنشئ موقعاً على الإنترنت لأمن تقنية المعلومات في المنظمة، تقوم بتحديثه يومياً.
- اجعل من نفسك «الصوت الواحد» في كلّ الأوقات، وفي كلّ مكان.

- أجب عن الأسئلة التي تتعلق بالأخبار الجيدة بشكل سريع وعن الأسئلة التي تتعلق بالأخبار السيئة بشكل أسرع.

البعد الثالث:

طوِّر «الرسالة»:

إعرف جمهورك ـ إعلم ما الذي يثير اهتمامهم. ألّف رسالةً مفادها «أن ما بداخلها هو من أجلهم» من وجهتي نظر كلٍّ من الأخبار السيئة والجيدة. وإذا كان كلٌّ من المساهمين أو الزبائن سيستفيدون من تحسينات الأمن فدعهم يعلموا بذلك. وإذا كانوا سيتأثرون بشكلٍ سلبيٍ مالياً أو قضائياً فأعلمهم بذلك أيضاً.

إن الرسائل الجيدة «تُعالجُ بوضوح» القضايا الجوهريةَ التي يواجهها المساهمون (سمعة المؤسسة، والتأثيرً المالي والنمو المستقبلي) والزبائن (تسرب المعلومات الخاصة بهم، والفقدان الكامل للمعلومات، وتشديد النفاذ إلى المعلومات).

إطّلع على الأمور التي يسألُ عنها الزبائن والمستثمرون لكي تستخدم نفس مصطلحاتهم. إجعل الرسالة مختصرة ومركزة، واستثنِ التواريخ المحددة، والقضايا قصيرة الأمد أو القضايا المالية التي لا تكون متأكداً منها.

عندما تكون الأخبار جيدة، أخبر الجميع عن السببِ الذي جعلَ الأمورَ تسيرُ بشكلٍ جيد، وعن الفوائدِ والمكاسبِ التي سَتُجنى. عند الأخبار السيئة حدِّد من الذي تأثَّر، ومن الذي لم يتأثر، وما هي الأسباب وراء ذلك، وما هي الحلول المتيسرة؟

البعد الرابع:

أدر «الرسالة»:

إن تحديدَ تواترِ وكيفيةِ وفرصِ إدخال التحديث لرسالتك، هي قرارات إدارية رئيسية. يمكن عادةً إصدار الإعلانات عن الأخبار الجيدة في أيِّ وقتٍ

لتلائمَ جدولَ كلِّ المعنيين. أما عند الأخبارِ السيئةِ فلا يوجد وقتٌ مناسبٌ أبداً لإخبار الزبائن والمساهمين بها. فمن الممكن توقيت إصدار الرسالة عندما تُصبحُ لديك معلوماتٌ دقيقةٌ لشرح ما حدثَ، ولماذا حدثَ، وما هي خططُ العملِ الإصلاحية التي بُدئت. إن الإعلانَ عن معلوماتٍ دقيقةٍ أفضل من عرض تكهنات مبنية على افتراضات متغيرة سريعة.

إذا اقتضى الأمر تقديم أي تحديثات، أخبر الجمهور متى سيتم تزويدهم بها، وبأي شكل (طريقة العرض، البريد الالكتروني، الرسالة الصوتية، الإعلان على الموقع في الإنترنت، . . . الخ).

قد يكون للعوامل الخارجية تأثيرٌ في مجالِ ومصادرِ أمن تقنية المعلومات التي يجب أن تُذكر إلى كلٍّ من المساهمين والزبائن أثناء تقديم العروض؛ إذ توجد حالات خارجة تماماً عن أيَّةِ سيناريوهات أو تخطيطٍ معقول، مثل هجمات 11 أيلول/سبتمبر عام 2001 على البنتاغون، ومركز نيويورك للتجارة العالمية.

الفصل الثالث

حماية المعلومات الخاصة بالزبون

تشارلز ريكس الرابع (IV)

جامعة الدفاع الوطني، الولايات المتحدة الأمريكية

المقدمة

إن حماية المعلومات الخاصة بالزبون أمرٌ حاسمٌ لنجاح المنظمة. لذا يتوجب على الشركات أن تمتلك خطة إستراتيجية لأمن المعلومات التي يزودها الزبائن بها بغية الحفاظ على عدد الزبائن الموجود وكسب زبائن جُدد. تقع هذه المسؤوليةُ على عاتقِ الشركة، فالشركة التي تعطي قيمةً مضافةً إلى الزبون، وتؤمن أفضل الوسائل نفعاً لفعل ذلك، سوف تفوز في السوق التنافسي.

إنه لأمرٌ واضحٌ أن حمايةَ المعلومات الخاصة بالزبون مهمةٌ صعبةٌ في المحيط التقني المتنامي والمتغير بسرعة. على أية حال، هذا هو التحدي الذي يتوجَّبُ على جميع الشركات القيام به لتتنافس بنجاح في عالم التجارة. وبالنتيجة، فإن على المدراء التنفيذيين وإدارة المنظمة مسؤوليةً ائتمانيةً تجاه حاملي أسهُمِهِم لزيادة قيمة الشركة. تزداد قيمة الشركة بازدياد عدد الزبائن، إلا أن إخفاقات الأمن تضعف من هذا المسعى.

يجاهد المدراءُ والتنفيذيون لتبريرِ نفقاتِ الأمنِ التي لن تعطي عائداً

فورياً على الاستثمار، نظراً إلى أن أمنَ تقنيةِ المعلومات هو لعبة خاسرة. يضاف إلى هذه الصعوبة التعقيدُ في تحديدِ الثغرات الموجودة في هذه البيئة الديناميكية وفي تحديد التهديدات المحتملة التي قد، وقد لا، تَكشِفُ عن نفسها. كذلك تَصعبُ موازنة المخاطر مع القيمة المكتسبة من الاستثمار في تقنيات أمن المعلومات، وإن المبالغةَ في أيٍّ من طرفي هذه المعادلة تسبب الفشل.

تمتدُّ حمايةُ البيانات الخاصة بالزبون إلى أبعد من مجرد علاقة الزبون بالشركة، إنها تصل إلى علاقة الشركة بالشركات الأخرى على طول سلسلة التزويد من أسواق التوزيع إلى الممّونين. وقد تؤدي إخفاقاتُ أمن المعلوماتِ إلى عواقبَ قانونيةٍ قد تُعطِّلُ قدرةَ الشركة على العمل. تتطلب إدارةُ مسؤوليةِ الأمن قيامَ الشركات بتصميم خططٍ إستراتيجيةٍ لتأمين المعلومات على أن تتصف بالديناميكية في طبيعتها لتَتناسب مع الساحةِ التقنيةِ دائمةِ التطور. تربط هذه الخططُ الإستراتيجيةُ بالإجراءاتِ الوقائيةِ الفاعلةِ التي يجب أن تكون مرنةً لتجاري البيئة المتغيرة بسرعة.

تحديد المعلومات الخاصة بالزبون

ما هي المعلومات الخاصة بالزبون؟ إنها جميع المعلومات التي تحصلُ عليها المنظمة من أيِّ تفاعلٍ مع الزبون القائم أو المحتمل، بالإضافة إلى معلومات الزبون التي زُوِّدت من مصدرٍ خارجي. قد تتضمنُ القائمة الجزئيةُ لهذه المعلومات ما يلي: الاسم، ومعلومات الضمان الاجتماعي، ورقم الهاتف، والعنوان، والعمر، والجنس، والحالة الاجتماعية، والسلالة، والعرق، والتعليم، والمعلومات الائتمانية، والدخل، والمعلومات الأسرية وبيانات الوظيفة.

يحتفظُ العديُد من المنظماتِ بهذا النوعِ من المعلوماتِ. فعلى سبيل المثال: تخزِّنُ دوائرُ دخلِ الحكومةِ من الضرائبِ (IRS) كميةً هائلةً من المعلومات عن زبائنها (أي دافعو الضرائب). تحصل (IRS) على هذه المعلومات من أصحاب العمل. وعلى الرغم من أن (IRS) لم تحصل على هذه المعلومات مباشرةً من الزبون، إلا أنها تتحملُ مسؤوليةَ أمن هذه المعلومات.

الثغرات والتهديدات

إن «الثغرة» في مصطلحات الإنسان العادي هي خلل في التجهيزات، أو البرمجيات لحاسوب أو لنظام الشبكة، أو في بوابة الدخول إلى نظام الشبكة أو الحاسوب. في الحقيقةِ تكون الثغراتُ مطلوبةً لتسهيل الاتصال بين حاسوبين أو أكثر. فإذا اتصلتَ مع حاسوبٍ آخر، فأنت بالنتيجة تُجري نوعاً من التغيير في نظام الحاسوب الآخر. وبينما يعدُّ هذا العمل مرغوباً، إلا أنه قد يُستغلُّ أيضاً.

إذا ما استغلَّتِ الثغرة فإنها ستصبحُ تهديداً لنظام الحاسوب أو الشبكة. قد يكون التهديدُ أيضاً شخصاً أو نظاماً حاسوبياً خبيثاً يسعى إلى إحداث الضرر لنظام حاسوبي آخر أو لشبكة أخرى.

بينما ستتواجدُ دائماً ثغراتٌ في شبكات وأنظمة الحاسوب، إلا أنه قد لا يوجد دائماً تهديد. من الضروري الإشارةُ إلى أن الذي قد لا يكون ثغرةً أو تهديداً في الوقت الحالي، قد لا يبقى على هذه الحال في المستقبل، فقد تظهر فيما بعد فجأةً ثغرةٌ غير موجودة على أنها تهديدٌ نتيجةً لتقنياتٍ حديثةٍ مثل تحديثات البرمجيات، والأجهزة التي تضاف إلى الأنظمة المربوطة على الشبكة.

ثروة المساهم

تزدهرُ سوقُ التجارة الالكترونية نتيجةً للعلاقات المترابطة عبر الشبكات. إن الشركات التي فشلت في تبنّي التجارة الالكترونية قد استُبدِلَت أو أنها تتخبط في المياه لتبقى طافية. لقد غيَّرَ التنافسُ العالمي اقتصادَ جميع الأسواق. فلم يعد لدى الشركات خيارُ العودةِ إلى طرقها القديمةِ في ممارسة الأعمال. فأنت لم تعد قادراً على إعادة العفريت إلى القمقم، فقد فتح صندوق «باندورا» للتو[*].

توجد علاقةٌ تناغميةٌ بين الزبائن والمستثمرين، فكلما اكتسبت الشركةُ زبائن

(*) أي فتح الصندوق المليء بالشر، وانتشر هذا الشر في كل مكان، ولم يعد بالإمكان إعادته إلى داخل الصندوق. هذا تعبير من تعابير الأساطير الإغريقية، حيث «بندورا» كانت المرأة الأولى على الأرض وهي التي كسرت الجرة المليئة بالشر الذي انتشر في الأرض ولم يعد بالإمكان لملمته.

ازدادت قيمتها، وكلما ازدادت قيمتها أصبحت أكثرَ جاذبيةً، من حيث الربحية، للمستثمرين. لذلك فعلى إدارة الشركة وتنفيذييها مسؤوليةٌ ائتمانيةٌ تتلخصُ في اتخاذ القرارات التي تزيدُ من قيمة الشركة.

تسبب إخفاقات أمن المعلومات دماراً لهذه العلاقة بين الزبائن والمستثمرين. لسوءِ الحظِّ، إن العديدَ من الشركات لا تتبنّى إجراءات الأمنِ إلا بعد وقوع الضرر. تظهر هذه الإخفاقات عادةً على الشكل التالي: هجمات الحرمان من الخدمة، والفيروسات ومشاكل البريد الإلكتروني. قد تستمر هذه القائمة وتستمر، إلا أن الهجمات في الكثير من الأحيان قد تمضي بدون أن تلاحظ، في بادىء الأمر على الأقل. في بعض الأحيان ولسوء الحظ، تكون الهجمات غير الملاحظة الأكثرَ إيذاءً، كما في المثال الآتي:

في عام 2001م، تلاعب أبراهام عبد الله، البالغ من العمر 32 عاماً، على أكثرِ من 200 شخص من لائحة (Forbes) «أغنى 400 شخص في أمريكا» عن طريق سرقة هويتهم الرقمية. لقد جمع السيد أبراهام المعلومات عن هؤلاء الأشخاص باستخدام حاسوبٍ متاحٍ للعامة موجود في مكتبةٍ في بروكلين ـ نيويورك. وقد نجح في قرصنة قواعدَ بياناتٍ تعود إلى بعضِ أكثرِ شركاتِ الائتمانِ أهميةً في العالم وتحتوي على معلومات شخصية. استخدم هذه المعلومات لفتح حسابات الدائنين بشكلٍ مخادع، وبالنهاية سرق ما يزيد على 80 مليون دولار. لقد احتاجت السلطات إلى أكثر من ستة أشهرٍ كي تلقي القبض على أبراهام. وجدت السلطات في حوزته أكثرَ من 800 بطاقة ائتمان احتيالية و20,000 بطاقة فارغة.

إن هجمةً بهذهِ الضخامة قد تُدمِّر الشركةَ، إذ إن الإخفاقات الأمنية للشركات تؤدي إلى العديد من المضاعفات الخطيرة، وفي مقدِّمتها عادةً فقدانٌ واضحٌ للزبائن. يُعلَم زبائن اليوم بسرعةٍ بمضاعفاتِ إجراءاتِ الأمنِ الواهنةِ، فإذا أصبح واحدٌ من زبائنك هدفاً لمثل هذه الهجمةِ بسببِ إجراءات أمنٍ غير كافيةٍ من قبل شركتك، فمن الأرجح أنَّهُ سيقطع علاقته معك، وعليه قد تتضاءل قيمة الشركةِ وتفشلُ في النهاية.

قد يبدو أنه لتجنب حدوث هذا السيناريو يكفي قيامُ المدراءِ والتنفيذيين برفع شعارٍ مفاده أنهم «سيحمون» أمنَ المعلومات. لسوء الحظ، إنَّ المسألةَ

ليست بهذه البساطة، فهي ليست فقط امتلاكَ الأمنِ أو عدمه. أولاً: إن من المستحيل تقريباً إزالةَ جميعِ الثغرات، إنه اقتراحٌ مستحيلٌ لأنَّ التقنيةَ تتطور باستمرار. تُصمَّمُ أنظمةُ الشبَكةِ لتتصل مع أنظمةٍ أخرى، وطالما أن الأنظمةَ تتصل مع بعضها البعض، فإنها سوف تسبب ثغراتٍ لأن عمليةَ الاتصال بحد ذاتها تتطلبُ تملك كل نظام القدرة على تبادل المعلومات مع الأنظمة الأخرى. يضافُ إلى ذلك أن الاستثمارَ في أمنِ التقنيةِ غالٍ إلى أبعد حد. لا تُرجِعُ هذه الاستثماراتُ عادةً عائداً ملموساً فورياً، بل على العكسِ تماماً فعائداتها عادةً سلبيةٌ جاعلةً هذا الاستثمار غير جذاب.

على الرغم من أن التكلفةَ الماليةَ لحماية أنظمة تقنية المعلومات، وحمايةِ المعلومات التي تحويها، عاليةٌ واقتراح رصدها هو اقتراح غالٍ، إلا أنها ضرورية. إذ قد يكون اختيار عدم الحماية مكلفاً أكثر في النهاية لأن الزبائن عندها ستُوقفُ التعاملَ مع الشركة. إن إدراك أن عدم القيام بشيء ليس بخيارٍ، يجعلُ الشركةَ تعمل على إعداد خطة إستراتيجية لتدفع إلى الأمام حماية أصولها المعلوماتية.

من الضروري منذ البداية إدراك أن الاستثمار في أمن تقنية المعلومات سيتطلب موارد مالية عظيمة، وأن العائَد على الاستثمار غالباً غير ملموس. إن اتخاذ طريقة متقدمة في كل الاتجاهات لتأمين المعلومات تعطي نتائج مذهلة على أية حال.

لقد بات من المسلّم به، في ساحة العلاقات بين الشركات، أنَّ أمنَ التقنية هو من متممات النجاح. تبدأ الشركاتُ بالتركيز على حماية أصولها، وتُدركُ عند قيامها بذلك أن الثغرات تتواجد نتيجة قيامها بتعاملات مع شركات أخرى. إن الابتكارات التقنية التي وجدت مكانها سريعاً في السوق، مثل تبادل البيانات الالكتروني (EDI) وأنظمة تخطيط موارد المؤسسة (ERP) وأنظمة إدارة العلاقة مع الزبون (CRM)، قد أجبرت الشركات على دمج شركائها في استراتيجيات أمنها. يجب أن تملك الشركات شكلاً من الاطمئنان إلى أن لشركائها في السوق آلياتِ أمنٍ جاهزة كي تتجنب التهديدات المحتملة، وبالتالي تخفف الثغرات القائمة بين الشركات المتشابكة تقنياً.

عادةً ما تمضي هذه العلاقة المتشابكة بين الشركات بدون إشكالاتٍ إلى

أن يخفقَ شيء ما. يتواصل المزودون إجمالاً من خلال نظام (EDI) مع شركات التصنيع أو مزودي الخدمة. لقد مكَّنَ هذا الاتصالُ الالكترونيُ الشركات من تخفيضِ النفقاتِ غير المباشرة المرتبطة بتنظيم الجرد، وتخصيص المؤونة، والشحن. . الخ. ويغطي نظامُ (EDI) عادةً عدة طبقاتٍ على طول سلسلة التزويد. إن أنظمةَ تخطيط موارد المؤسسة (ERP) الموجودة في شركات التصنيع أو تزويد الخدمة قد مكنتها من جعل عملياتها أقربَ إلى الكمال، ضامنين بأن الموارد متوفرة لإدارة العمليات بدون توقف. ترتبط كذلك أنظمة (ERP & EDI) بأسواق توزيع البضائع والخدمات التي تقوم بها الشركة. وفي بعض الأحيان يرتبط الزبون بأسواق التوزيع مباشرة من خلال تقنيات (CRM). وكما شُرِحَ سابقاً، قد يتواصل الجميعُ عبر الابتكار التقني، على طول سلسلة التزويد الكاملة ابتداءً من الزبون حتى المزود. تسبب هذه العلاقة المترابطة العديدَ من الثغرات. إن هذه الثغرات لا تُستَغَلُّ جميعها من قبل التهديدات. يتوجب على الشركات امتلاك القدرة على تحديد الثغرات الخطيرة على عملياتها المتواصلة فتقوم أولاً بحمايتها، بينما تحمى الثغرات الأخرى، الأقل خطراً، في ما بعد.

زيادة عدد الزبائن والحفاظ عليهم

يميل الزبائنُ إلى التعامل مع الشركات ذات السمعةِ الحسنة، التي تقدم المنتجات والخدمات التي يطلبونها بسعرٍ معقول، والتي تَحترمُ رغبات الآخرين، وتتعامل مع المستخدم بشكلٍ ودِّي. يستطيع الزبائن، في بيئة السوق العالمية الحالية، التعاملَ افتراضياً مع أيِّ شركة في العالم. لم يكن هذا ممكناً في الماضي، فلقد كانت الشركات معزولة عن المنافسة العالمية بفعل الجغرافيا، والعملات، واللغات. إن ذلك لم يعد موجوداً في سوق اليوم.

لكي تكتسب سمعةً حسنةً يجبُ على الشركةِ النجاح في أمرين: أن تعرض أجودَ المنتجاتِ أو الخدماتِ وأن تملك سجلَّ أداءٍ معترف به. في عصر الإنترنت، تنتشر الإخفاقات في هذين المجالين كالحريق الهائل، فمن الممكن الوصول إلى سجلات الشركة بلمسة زر. إن انفتاحَ السوقِ العالمية قد عَزَّزَ المنافسةَ القوية بين الشركات، إذ يستطيع الزبائنُ الآنَ المقارنةَ بين منتجات

العديد من الشركات للحصول على السعر الأكثر تنافساً. تؤثر كذلك تجربة الشراء وسهولتها في قناعات الزبون. إن تضافر كلٍّ هذه المعاييرِ قد يثبِّتُ البيعَ أو يوقفه. إذا فشلت الشركة في أي أمرٍ من هذه الأمور، فإن إمكانيةَ زيادة عدد الزبائن والحفاظ عليهم تصبحُ مثيرةً للجدل.

يجب أن يَطمئنَّ الزبائنُ إلى أن معلوماتهم مهمةٌ للشركةِ وسوف تُحفَظُ كذلك. على سبيل المثال: في حالة الصفقة التي تُبرَم من خلال شبكة الإنترنت، من الضروري امتلاك الشركة آليات أمنية تحمي بطاقة ائتمان الزبون أثناء الإرسال عبر الإنترنت. إن إجراءات الحماية مثل الحواسيب المخدة الآمنة وجلسات الإنترنت التي تضمن الخصوصية، قد تسهّل هذا الهدف. فور الحصول على المعلومات من الزبون يجب أن توضع تحت الحماية، فثقة الزبون هي الهدف.

المسؤولية الحرفية

لا بد لإخفاقات الأمن من الحدوث، فالشركات التي لم تقع في قبضات الاعتداء على أمن معلوماتها نادرة. إن مستخدمي الحاسوب الشخصي، أيضاً، على درايةٍ ببعض التبعات المدمرة بسبب إجراءات الحماية غير الكافية. تُدمِّرُ فيروسات الحاسوب أنظمةَ الحاسوبِ مدخلةً الديدانَ وأحصنة طروادة، مخربةً رموز الحاسوب ومسببةً بذلك ساعاتٍ من الإحباط. إن تكلفة هذه الثغرات غالية بالنسبة إلى الحاسب الواحد، ولكنها تصبح أُسيِة في البنى التحتية المتشابكة الهائلة. قد تخسر بعض المؤسسات ملايين الدولارات يومياً بسبب هذه الاعتداءات.

تواجه المنظمات في كلٍّ من القطاع العام والخاص تحدّياً آخر أيضاً عندما تُستغلُّ ثغرات نظامها. يتمثل هذا التحدي في السؤال الهامِّ: هل من الأفضل إعلام السلطات بالهجمة، وهل تُنشرُ المعلومات بخصوص الهجمة على العامة؟

إن تقديمَ تقريرٍ حول حوادث أمن المعلومات إلى السلطات أمرٌ حساسٌ بطبيعته. ولكن من جهة، تحتاج الشركةُ إلى المساعدةِ من كلِّ الجهات وإلى عدمِ إفشاءِ أسرارها، إلا أن السلطات من جهة أخرى ملزمةٌ قانونياً بتسجيل

التقريرِ حولَ الحادث والإعلام عنه من أجل أهدافِ الرقابةِ والتحقيق. إن مكتب المباحث الفيدرالي (FBI)، في الولايات المتحدة على سبيل المثال، هو الجهة المنوط بها التحقيق في حوادث الجرائم المعلوماتية في القطاع الخاص. ويُوظِّفُ القطاعُ الخاص أيضاً فرقاً سريةً للتحقيق القضائي في الجرائم المعلوماتية كي تساعدَ في تذليل الصعوبات وحمايةِ البنية التحتية. ينتفعُ أيضاً القطاعُ العامُّ من خدمات الـ (FBI)، ولكن المنظمات الحكومية الأمريكية التي لعملها صلة بالأمن الوطني يجب أن تُخبِرَ أيضاً وكالة الأمن الوطنية (NSA).

لقد تم تأسيس العديد من فرق الاستجابة لطوارئ الحاسوب (CERTs) في جميع أنحاء العالم، لتساعد المنظمات في العودة إلى الوضع السويِّ من بعد الاعتداءات على الحاسوب. إن كلاًّ من القطاعين العام والخاص يستفيدان من خدمات (CERTs). إنها مفيدةٌ للغاية أثناء الاعتداءات الأولية على الأنظمة الآلية. ابتدعت فرق (CERTs) تقنيات إثباتٍ عديدةٍ لتحديد المعتدي وتقديمِ الإرشادات حولَ إبعادِ التهديد الحالي.

إن الإعلانَ عن الاعتداءات والاختراقات في أمن المعلومات إلى العامة هو أمرٌ حساسٌ أيضاً. إذ قد يؤدي إعلانُ إخفاقات الأمنِ إلى آثارٍ وخيمةٍ. فبينما يوجد من يقول بأن على المنظمة مسؤوليةً حرفيةً وعليها أن تُبلِّغَ عن هذه الاختراقاتِ من أجل حماية مصالح الزبون، يوجد كذلك من يقول بعدمِ الأخذِ بهذه الخططِ الإخبارية. إن الإبلاغَ عن ثغرات الأمن بحد ذاته، قد يؤدي إلى تصاعدٍ في الهجمات المماثلة على الثغرة نفسها.

يجب على الشركة أيضاً أن تأخذَ في حسبانها بأن الإبلاغَ عن خللٍ أمني قد يؤدي إلى خسارةِ الزبونِ وفقدانِ ثقة المستثمر. فإذا ما تبخَّرت ثقةُ المستثمرِ والزبون، فإن الشركة لن تكون فقط مضطرةً إلى الإسراع في ترقيع الثقوبِ الموجودة في أمنها، وإنما ستضطَّرُ أيضاً إلى إعادة طمأنةِ الزبائن والمستثمرين بأنه يجري اتخاذ الإجراءات المضادة لإيقاف الهجمات القائمة وتلك المقبلة. إن ردود أفعال الزبائن والمستثمرين العفوية، ستضاعفُ وتطيلُ الصعوبات.

إن على الشركات التي تَرتَبِطُ مع شركاء بسلسلة التزويد، مسؤوليةَ إعلام شركائهم بالخللِ الأمني الحاصلِ بُغيةَ الحد من انتشار ثغرات الأمن المدمرة المحتملة إلى شركائهم.

تبيّن المقالة «دراسة حالةِ مشهدٍ محتمل»، "Case Study Scenario, the iPremier Company (A): «Denial of Service Attack» التي نشرها قسم إدارة الأعمال في جامعة هارفرد عن حالةِ شركةٍ مفترضةٍ تعرضت للاختراق المعروف بـ «الحرمان من الخدمة» (DOS)، الفوضى التي تنتج عند إخفاق أمن المعلومات داخل الشركة. على الرغم من أن هذا السيناريو ليس حدثاً فعلياً، إلا أن الأفعال المتخذة في هذه الدراسة تشبه بشكل ملفت للنظر الأفعال التي تقوم بها الشركات خلال الهجمة الأولى على (أمن معلوماتها). من المستحسن الحصول على نسخة من هذه الدراسة كوثيقة تدريبية لأجل جميع المستويات داخل المنظمة (Austin, 2001).

أمن المعلومات لعبة خاسرة

يُعدُّ الأمر جيداً من المنظور الأمني عندما لا يحدث **شيء**، إلا أن تبرير **عدم حدوث شيء** هو أمر غير مقنع للإدارة العليا، والمدراءِ التنفيذيين، وأعضاء مجلس الإدارة، والمساهمين. وذلك لأننا تعلمنا عرفاً أن النجاحَ يعني عادة أن **شيئاً ما** قد حدث. إن إعادة تنظيم أدوات القياس لدينا من أجل برهان أن حالة **عدم حدوث شيء** هي فعلاً جيدة، لهو أمر صعب في أحسن الأحوال. تواجه وزارة الأمن الوطني الأمريكية (DHS) عائقاً مشابهاً. إذا لم يحدث شيء، فإن الوزارة (DHS) ناجحة؟ من الصعب قبول هذا المعتقد لأن النجاح في المفهوم التقليدي يعرَّفُ عادة على أنه التحسن في مؤشرات مالية قابلة للقياس.

على أيَّةِ حال، يمكن الحصول على مؤشراتٍ قابلةٍ للقياس إذا كانت لدينا وضعيةُ أمنِ معلوماتٍ قوية. وبرغم أن المؤشرات القابلة للتكميم في حالة أمن المعلومات هذه ليست من النوع المالي، إلا أن **عدد الهجمات** الكامنة التي تم صدها بنجاح تقاس رقمياً. وإذا كانت آليات أمن المعلومات جيدة فهي قادرة على جمع المعلومات حول هذه الهجمات المحتملة. ويجب أن تركِّز تقارير حالة أمن المعلومات على كلٍّ من نجاحاتِ وإخفاقاتِ عملياتِ الدفاعِ هذه.

إن عمليةَ الإبقاءِ على وضعيةِ أمنٍ قويَّةٍ مهمةٌ لا تنتهي أبداً، فالمحيط التقني محيطٌ ديناميكيٌ، وبالتالي فإن آليات الأمن يجب أن تتطور وتتغير مع التقنيات البازغة. سيمتعض كلٌّ من المدراء التنفيذيين وأعضاء مجلس الإدارة من

الاستثمار في أمن البنية التحتية الذي لا ينتهي. على أية حال هذا هو الأمن، وهذا هو اسم اللعبة.

لقد غيَّرَ التطورُ التقني مظهرَ السوق، فلقد مكَّنَ الشركات من المنافسة في أسواق لم يسبق لها أن وجدت من قبل، وبطرقٍ لم يسبق حتى تخيلها منذ عقدٍ مضى. يستطيع الموظفون الآن أن يعملوا في بيوتهم عن طريق الحاسوب بدون الحاجةِ إلى وجود مكتبٍ في مركز المدينة التجاري. وبإمكان الموظفين أيضاً أن يعملوا افتراضياً من أيِّ مكانٍ في العالم باستعمال الحاسوب المحمول أو حتى المساعد الرقمي الشخصي (PDA) الذي هو بحجم كفِّ يدك. ولكن مع هذه المرونة تأتي أيضاً الثغرات والزيادة في التهديدات.

تكون البنية التحتية لأمن المعلومات جيدةً بقدر ما تكون أدواتها المعتمدة كذلك. بكلماتٍ أخرى، تخيَّل بأنك تملك حاسوباً محمولاً مرتبطاً بحاسوبٍ مخدِّمٍ يؤمن شبكةً افتراضيةً خاصةً (VPN) مزودةً بإمكانياتٍ للتعمية (للتشفير) تسمح لك بأمان إقامة اتصالٍ نفقيٍّ آمنٍ بشبكة شركتك مع شهادات توثيق الهوية الخاصة بحاسوبك. إن تقنيةَ الأمن هذه قويةٌ بحسب أغلب المعايير، لكن تخيل استخدام حاسوبك المحمول عندما تكون في دولةٍ أخرى مستعملاً خطوطَ اتصالاتٍ قد تكون خاضعةً للمراقبةِ من قبل أطرافٍ أخرى مهتمة. إن عقد الصفقاتِ عبر هذه الخطوط سيكون خاضعاً للتنصُّتِ، ومن الممكن أن يكون معرضاً حتى للاستغلال. إن احتمالَ حدوث خللٍ أمني أمرٌ بديهي.

تخيل مجدداً الحاسوبَ المحمولَ نفسَه مع آلياتٍ لأمن المعلومات ذاتها قد سُرِقَ من قبل سارقٍ ما. إذا كانت لدى هذا السارق نيةٌ خبيثةٌ ومعرفةٌ عمليةٌ بالحاسوب، فمن المحتمل أيضاً أن تخترق آليات الأمن. إذاً تُمَثِّلُ الأداةُ المعتمدةُ، الحاسوب المحمول في هذه الحالة، تهديداً خطيراً على البنية التحتية للأمن، رغم أنها تبدو قوية ظاهرياً.

دعنا نتوسع في هذا الموضوع أكثر قليلاً، تخيل زبوناً ما يدير عملاً مع شركتك، عادةً قد لا يكون الزبون ضليعاً في الحاسوب، ولكنه يعلم ما يكفي لإنجاز صفقة تجارية عبر الإنترنت. من ناحية ثانية لا يملك الزبون جدارَ «نارٍ» في حاسوبه. يستخدم الزبون اتصالاً ذا حزمةٍ عريضةٍ من الترددات، وبذلك فهو

متصلٌ بالإنترنت بشكلٍ مستمر، كما أنه قد اعتاد على ترك حاسوبه في حالة عملٍ دائم باستثناء أثناء وقت حدوث العواصف. إنه قد لا يعلم بأن قرصاناً (Hacker) قد اكتشف رسائله الموجودة في الحاسوب وتتبعها وأنه قد حمَّل برنامجاً على نظام التشغيل لديه يسمح للقرصان سَرِقَةَ تعاملات الزبون حسب هواه. وبما أن الزبونَ قد أجرى تعاملاتٍ مع شبكتك، فإن طريقاً واضحاً إلى بياناتك الحسَّاسة قد فُتِحَ للقرصان. يقوم القرصانُ بسرقةِ جلسة الزبون ويبدأ باستغلال أنظمة حاسوب شركتك. بالاعتماد على آليات الأمن الموجودة في شركتك، فإنك قد تلاحظ أو لا تلاحظ الاعتداء، وقد تكون قادراً وقد لا تكون قادراً على التصدي له.

إن التكلفةَ المنخفضةَ لتنصيب الشبكات المحلية اللاسلكية (WLANS) قد جعلت هذه الشبكات بديلاً جذاباً للشركات. نظراً إلى أن العديد من الشركات تستخدم مساحاتٍ مكتبيةً مستأجرةً، وباعتبار أنها معتادة على التنقل إلى مساحات جديدة كل سنتين، فإن البنى التحتية لشبكات (WLAN) تُعدُّ مريحةً وفعالةً جداً من حيث كلفتها المنخفضة، كما إنها بديلٌ مرنٌ عن البنية التحتية للشبكة المحلية السلكية الدائمة (LAN) غاليةِ التنصيبِ. إلا أن الشبكات اللاسلكية تحتوي ثغراتٍ أمنيةً خطيرةً إلى أبعد الحدود؛ إذ لم تعد الشركة قادرة على حماية شبكتها ببساطة من الاستخدام المحظور عن طريق استخدام تقنيات أمن المعلومات المادية أو الملموسة مثل حراس الأمن والأبواب المقفلة. يتوجب على الشركة الآن أن تحمي الموجات اللاسلكية التي حلت محل البنية التحتية للشبكة السلكية. إن هذا مشابه «لوضع مأخذٍ لشبكتك السلكية (Ethernet) في موقف السيارات لشركتك!!» (Reid and Seide, 2003). يجب حماية البنية التحتية للشبكله اللاسكية (WLAN) بنفس العزم الذي عقد على حماية أي شبكةٍ أخرى.

يتضمن أمن المعلوماتِ على شبكات الحاسوب العديد من الشراكِ والقضايا. إذ قد تعاني المنظماتُ ردود الأفعال العفوية بعد استغلالهم باعتداء ما، فقد تقع الشركاتُ في فخِّ الإنفاق المفرط على أمن الحاسوب. فقد تستثمر الشركات التي لا تمتلك خبرةً كافيةً بشكل كبير في إجراءات الأمن مما يجعلها تتصدى بجدارة للتهديد الحالي، لتجد بعد ستة أشهر أن إجراءات الأمن هذه غير قادرةٍ على التصدي لهجماتٍ جديدة. وينتجُ من ذلك استنزافها ميزانياتِ

مواردها بشكلٍ كبيرٍ مما يجعل الاستثمارَ مستحيلاً في تقنيات أمنٍ أحدث لتحسين دفاعاتها. وسيخامرها شعورٌ بأنها قد قامت بشراء قارب فيه ثقب تصب بداخله المال. وحتى لو لم تكن الموارد المالية عثرة، إلا أن جميع أموال العالم قد لا تحقق النتائج المرغوبة بدون خطةٍ إستراتيجيةٍ طويلة الأمد لأمن المعلومات.

لا يزال هناك شركٌ أو فخٌ آخر تقع فيه الشركات عادةً، ألا وهو الحسُّ الخاطئ بأن أمنها مُطَمئن. يُعرفُ هذا الفخُّ بـ «متلازمة الحادي عشر من أيلول/ سبتمبر» (September 11th Syndrome). تفترض الشركات في هذا الفخ أنه ونظراً إلى أنها لم تعانِ أبداً من الاعتداء في الماضي، فهي محميةٌ من الاعتداءات في المستقبل. قد تعتقدُ كذلك بأن أنظمةَ حواسيبها لا تحتوي على بيانات زبونٍ حساسةٍ أو بياناتٍ متعلقةٍ بطريقةِ التشغيل، ولكن في الحقيقة إن لديها العديد من سجلات البيانات الموجودة في عملياتها التجارية اليومية والتشغيلية ولكنها لا تدركها. بشكل عام إن الأمهات والآباء البسطاء معرضون مثلهم في ذلك مثل: الشركات الـ 500 الأكثر ثراءً في العالم والموجودين في لائحة مجلة *Fortune*.

لا تنسى أن بعضاً من أكثر الاعتداءات تدميراً هي تلك التي تمضي بدون أن تلاحظ. قد يستغلُّ القراصنةُ الخبثاءُ أنظمةَ الشبكات الحاسوبية جامعين بيانات الزبون الحساسة بشكل مستمر. وقد تكون انعكاساتُ هذه الهجمة هائلةً ويتعذر إصلاحها، ومن المحتمل أن تنهار الشركة في يوم واحد حسب طبيعة ومدى الاعتداء.

تتطور كلٌّ من التهديدات والثغرات وتنمو بشكلٍ مستمر. إن مجاراةَ التقنيات البازغة أمرٌ مليءٌ بالتحدي، ولكن مجاراةَ التهديدات التي تكون غير معروفة هو أيضاً أمرٌ أكثر صعوبة. يأتي القراصنةُ بأشكالٍ عديدةٍ ابتداء من سن 12 سنة المؤذي، المعروف بالطفل الصغير (Kiddy)، إلى القرصان أو الإرهابي المحترف المثقف والمتعلم الذي يمتلك نوايا خبيثة. إن حجم الدهاء غير محدود، ولكن لا بد من التمييز بين نوعين من التهديدات، فهي إما أن تكون تهديدات خارجية أو داخلية.

إن الانطباع السائد هو أن التهديدات الخارجية هي الأكثر اختراقاً، إلا أن

هذا الادعاء خاطئٌ جداً، فالتهديدات الأكثر شيوعاً تأتي من مصادر داخلية. يمثل كلُّ شخص داخل منظمتك، بما في ذلك كبار المدراء التنفيذيين، ومدراء الشبكة، وموظفو خدمة الزبون، والطاقم الإداري، وأطقم المحافظة على الحدائق، وعمال التنظيف، تهديداتٍ داخلية. يتمتع العديد من هؤلاء الموظفين بوصول مباح إلى مصادر معلومات الزبون. وبينما قد تزيل آليات التحكم بالدخول العديد من التهديدات الداخلية إلا أن بعضاً من الموظفين سيبقى يتمتع بالوصول الكامل إلى البيانات المخزنة على أنظمة حاسوب الشركة. رغم أن هذا غير مرغوب، لكنه في الوقت ذاته لا يمكن تجنبه. على سبيل المثال: يتمتع مدراء الشبكة في العديد من الشركات بالنفاذ الكامل إلى جميع البيانات. إنهم يحتاجون عادة إلى هذا النفاذ لضرورات العمل للتأكد من أن العمليات اليومية للشركة ممكنة. ولكن إلى أيٍّ مدى يكون مدير شبكة شركتك جديراً بالثقة؟

إن فكرةَ التهديد الداخلي هي فكرةٌ مقيتةٌ ومستهجنةٌ من كلِّ الأوجه. يؤثر إدراجُ هذا التهديد في كلٍّ من الثقافة، والجو ونظام القيم للمنظمة وحتى العظم. لن ينظر الموظفون باستحسانٍ إلى المراقبة الدائمة لنشاطاتهم اليومية. وسيشعر الموظفون وكأنهم لا يدينون للشركة بأيّ مشاعر الولاء إذا كانت الشركة نفسهُا لا تثق بهم كفايةً لينجزوا عملهم بسرية وثقة. مع ذلك فإن الشركةَ واقعةٌ بين نارين، لأن الفشلَ في مراقبة نشاطات موظفيها هو مسؤوليةٌ قانونيةٌ كبيرةٌ.

تثير المصادر الخارجية تهديداً أصغر، ولكنه ليس أقل كراهةً. إذ تواجه التهديدات الخارجية تحديات كبيرة في إحراز النفاذ إلى أنظمة الحاسوب لأنها لا تمتلك ميِّزة الاطّلاع على ما يجري من داخل الشركة. تتطلبُ أيُّ آليةٍ أمنيةٍ مطبقةٍ على نظام الحاسوب وقتاً لِتُهزم. لذلك يتجنبُ القراصنةُ أحياناً الأنظمةَ التي تتطلبُ تكريس جزءٍ كبيرٍ من وقتهم لتحقيق الاختراق، وبالطبع يكون تدمير الأنظمة ذات الحماية الواهنة أسهلَ بكثير. في الواقع إذاً، المسار الأقل مقاومةً للاختراق هو الأكثر ربحاً للقرصان الخبيث.

مثلما توجد فروقٌ بين التهديدات الداخلية والخارجية، توجد كذلك مفارقاتٌ بين أهداف التهديدات المختلفة. فقد ينوي بعضُ القراصنةِ أن يعطلوا

فقط قدرة الشركة على إدارة العمل، وكمثال على هذا الاعتداء «هجمة الحرمان من الخدمة الموزعة» (DoS) التي تعيق قدرة الحاسوب على معالجة التعليمات، وبالتالي تخفف من قدرته على تأدية العمليات الحساسة، وربما تجبرُ الشبكةَ على التوقف. قد يسعى البعض الآخر من القراصنة ببساطة إلى السطو على الشبكة لتصفُّح المصادر من أجل كسب الاعترافِ بتفوقهم من قبل القراصنة الآخرين. إلا أَن بعضَ القراصنة يهاجمون بخبثٍ أنظمة الحاسوب ليصلوا إلى البيانات الحساسة للزبون أو للشركة، مثل السجلات المالية ومعلومات بطاقة الائتمان، أو يسعون إلى إحداث ضررٍ خطير. من الواضح أن المعتدي الخبيث هو صاحب التهديد الأكثر خطورة بالنسبة إلى الشركة.

الخطُ الرفيعُ الفاصلُ بين الذكاءِ والحمقِ (في أمن المعلومات)

يحتوي الفيلم بعنوان «خزعة النخاع الشوكي» (This is Spinal Tap) على واحدةٍ من أفضل الحِكَم على مرِّ العصورِ وهي: «يوجد خيطٌ رفيعٌ بين الذكيِّ والأحمق» (Reiner, 1984). يعدُّ هذا السطر صحيحاً في عالم التجارة أيضاً، خاصةً في سياق أمن المعلومات وتأمينها. إن تحقيقَ التوازن بين الذكاء والحمق هو مسألةُ فنٍ أكثر من اعتبار ذلك علماً. من الضروري أن تحدد كلُّ شركةٍ بدقةٍ ما هو الشيء الأحمق وما هو الشيء الذكي.

ما هو الأمر الأحمق؟ إن إحدى الطرق لبداية عملية تحديد الأمر الأحمق هي العمل عكسياً، مثل ممارسة الهندسة العكسية بجميع أنواعها. حتى يكون نظام الحاسوب آمناً مئة بالمئة يجب أن لا يكون موصولاً، مئة بالمئة، لأي شبكة، وبالتالي فهو عديم الفائدة. يستنتج من ذلك أن هذا الحل لا يمتلك صفات الأمن المطلوبة. فإذا ما وَجَدَ الزبائن، والشركاء في سلسلة التزويد، أن من المستحيل الاتصال بالشركة، فإنهم سيكفون عن محاولاتهم وسيسعون إلى التعامل مع شركات أخرى.

لتحديد ما هو الأمر الذكي، يجب أن تعمل الشركة على تحديد مستوى الأمن الذي يزود الشركةَ بأفضل وضعيةٍ أمنيةٍ مع مستوى مقبول من المخاطر. تتضمنُ عملية إجراء تقييمٍ مفصَّلٍ لأثرِ المخاطر، النظر في المواصفات التقنية لبنية الشبكة التحتية وتوحيد تلك المعلومات مع متطلبات عمليات الشركة

الحالية. تشتملُ هذه المعلومات على متطلباتِ وظائف الشركة الاستثنائية، والمتطلبات التشغيلية، والكفاءات الجوهرية، ومهام الشركة، وإدراك مطالب الزبون. ثم يُقرنُ تحديدُ ثغرات البنية التحتية ويطابقُ بينه وتحديد التهديدات المهيمنة، وتدرسُ بعد ذلك مع المتطلبات التشغيلية.

تجمعُ هذه البيانات وتحللُ من خلال عملية تقييم أثرِ المخاطر. من الضروري أن يُمَثَّل أغلب، إن لم يكن جميع، خبراء الوحدات الوطنية في الشركة أثناء عمليات تقييم أثر المخاطر لكي تحدَّدَ وتصانَ المتطلباتُ التشغيليةُ والحاسمةُ والاستثنائيةُ اللازمة لضمان استمرار عمليات الشركة. تُقدَّرُ بعد ذلك الثغراتُ والتهديداتُ المحددة لتعيين أيٍّ منها يُمَثِّلُ الأولوية الأعلى. تُربَطُ هذه الأولوية عادةً بالمهام الحساسة لهذه الوحدات.

يجب أن تُعطَى الثغراتُ والتهديداتُ، التي إذا ما استغلت قد تجبر عمليات الشركة على الوقوف، الأولويةَ الأعلى، أما الثغراتُ والتهديداتُ التي تسبب تأثيراً أقلّ وأبسط، أو التي تكون غير محتملةِ الاستغلال، فتعطى أولويةً أدنى. بعدَ تحديدِ الأولوية المناسبة للثغرات والتهديدات، تُصمَّمُ استراتيجيات تقليل أو إزالة هذه الثغرات والتهديدات، مع الأخذ بعين الاعتبار التأثيراتُ الماليةُ المتعلقةُ بطرق العمل لتطبيق هذه الآليات الأمنية.

الموافقة الرسمية (على مستوى أمن الشركات)

من الواضح أن حمايةَ المعلومات وتأمينها، في اقتصادِ اليوم المُعولَم والالكتروني والمشبَّك أو المترابط، تثيرُ قضيةً هامةً لجميع المنظمات. لقد تم عقد العديد من المناقشات والمنتديات في كلٍّ من القطاع العام والقطاع الخاص، لا سيَّما حول التحدِّيات التي تواجهها المنظمات اليوم فيما يتعلق بالموضوع. إذا ما أخذنا بعين الاعتبار أن الشركات تواجه ثغرات خطيرة غالباً بسبب اتصالها بعضها بالبعض، فإن إجراءَ التعاملات الالكترونية مع الشركة التي لا توظف آليات أمنية قوية هو مسؤوليةٌ قانونيةٌ كبيرة.

إن واحداً من الاقتراحات التي برزت هو اقتراح وضع سلّم أو مؤشّر لمستوى أمن المعلومات للشركات. يكمن تصميم هذا السلّم بشكل مشابه لذلك المطبق لدى مؤسسة Underwriters Laboratories الأمريكية التي تصنف

الشركات تبعاً لجودة منتجاتها، ومن معاييرها: « إصدار وثيقةٍ تضمنُ أن الشركةَ تمتلكُ سياساتِ حكومةٍ وإجراءاتٍ تقنية للبنية التحتية تجعل تلك الشركة أكثر أمناً» (Beach, 2003). سيفيدُ سلّم مستوى الأمنِ هذا كَمُطَمئن للشركات الأخرى بأن هناك بعضاً من الركون إلى أن شركاءهم في سلسةِ التزويدِ آمنون، كما أنه قد يُطَمئِنُ الزبائنَ أيضاً بأن معلوماتهم محمية.

ستكون مهمَّةُ هذه الجهة الضامنة تقييمَ البنى التحتية للشركات تبعاً لتطور معايير التأمين والأمن. وقد تعمل هذه الجهة كذلك كدارِ مقاصّة لأفضل الممارسات في أمن المعلومات وتأمينها مساعدةً بذلك الشركات في تطبيق إستراتيجيات الأمن ضمن تدريجات مرحلية.

إن الحصولَ على الوثيقة سيكون عملاً اختيارياً تقوم به الشركةُ التي تطلب ترتيبها في تحقيق أمن المعلومات.

لن يكون للجهة الضامنة أيُّ دورٍ تنفيذي، ولكنها قد تعمل كجهةٍ تستطيع أن تمنح تقديراً لحالة الأمن مرتكزةً على التقنيات الموجودة لدى الشركة. يجب تعيينُ مدةٍ للرقابة الدورية على أمن المعلومات لضمان أنَّ الوثيقةَ لا تزال صالحة. إنَّ إعادةَ التوثيق بشكلٍ دوريٍ كلَّ سنتين بعد المدة الأولية هو أمرٌ مستحسن.

التبعات القانونية

إن المحافظةَ على المعلومات الخاصة بالزبون تحملُ معها مسؤوليةً قانونيةً هامة، فسجلات الزبون مسؤولية قانونية ضخمة بحد ذاتها. وبالإضافة إلى ذلك هي أيضاً أصولٌ لا يستهان بها. إن أحدَ أسباب جمع معلومات الزبون هو أنها ضروريةٌ لإجراء التعاملات الإلكترونية معه في المقام الأول، وقد تساعدُ الشركة في الحصول على تعاملٍ آخر من قبله في المستقبل.

يتوقَّعُ الزبائنُ تأمينَ مقدارٍ من الخصوصية والسِّرية عند التعامل مع كلا القطاعين العام والخاص. ويجب أن يُطَمأَنوا بأن معلوماتِهِم الحساسة لن ترسل إلى أطرافٍ أخرى. إن بعضاً من هذا التأمين قد ورد في «قانون الخصوصية لعام 1974م» في الولايات المتحدة مثلاً. لقد توسع القانون أكثر في الإشارة إلى حماية المعلومات الخاصة بالزبون، وسيجري تناولها بالتفصيلِ فيما بعد في هذا الكتاب.

تتضمن بعضُ القوانينِ الأمريكيةِ التي تتعلق بوجه الخصوص بحماية البيانات الخاصة بالزبون(*): قانون نتائج وأداء الحكومة لعام 1993م، وقانون تقليل الوثائق لعام 1995م، قانون (Clingercohen) لعام 1996م، قانون الألفية لحقوق النشر الرقمية لعام 1998م، وقانون تحسين أمن المعلومات الحكومية لعام 2000م، وقانون التوقيع الرقمي لعام 2000م، والقانون المنادي بالوطنية عام 2001م، وقانون الحكومة الالكترونية لعام 2002م، وقانون (Sarbanes-Oxley) لعام 2002م.

قد تؤدي إخفاقات الأمن ـ وهي كذلك على نحو متزايد ـ إلى رفع دعوى قضائية من قبل الزبون. قد تؤدي حمايةُ البيانات الخاصَّة بالزبون بشكلٍ غير كافٍ، مسببةً بذلك إخفاقات أمنية، إلى مسؤوليات قانونية من خلال المحاكم. ومن الضروري لتَجنُّبِ مثل هذه النتائج أن تباشر الشركات إلى وضع خطَّة عمل تنفيذية لتطبيق إستراتيجية تأمين المعلومات.

تصميم استراتيجية تأمين المعلومات

الآن وبعد أن أصبحتَ على درايةٍ بالثغراتِ والتهديداتِ وبنتائج اتخاذِ الإجراءاتِ أو عدمه، أنت بحاجةٍ إلى تصميم إستراتيجيةٍ تُدركُ متطلباتِ الشركةِ التشغيليةِ، وتُقرنُ هذه المتطلبات بالحاجة إلى حمايةِ أصول الشركة وزبائنها، ولتخفيفِ التعرُّضِ إلى الكيانات التي ترغب بتسبب الضرر.

تحتوي إستراتيجيةُ تأمينِ المعلومات على العديد من خططِ العملِ التنفيذية المستقلة والمتداخلة: خطة الشركة الإستراتيجية، وخطة العمليات الطارئة، وخطة العودة إلى الوضع السوي بعد الكارثة، وخطة أمن البنية التحتية.

أولاً: إن خطَّة الشركة الإستراتيجية هي خطةٌ متكاملة. ترسم هذه الخطةُ «خارطة طريق» ترشدُ الشركةَ في المستقبل. يجب أن تحتوي هذه الخطَّة على المعلومات التي تحدد المتطلبات والمبادرات المستقبلية، والكفاءات الجوهرية، والرؤية التي تُبَيِّنُ كيف ستستجيب الشركةُ لمطالب زبائنها، والتوقعات المالية،

(*) The Government Performance and Results Act of 1993, Paperwork Reduction Act of 1995, Clinger-Cohen Act of 1996, Digital Millennium Copyright Act of 1998, U.S.Government Information Security Reform Act of 2001, E-Government Act of 2002, and the Sarbanes-Oxley Act of 2002.

والأدوار التي تلعبها البنى الإدارية، وتوقعات المساهمين، والطريقة التي ستتبعها الشركة لتكامل هذه التوقعات مع أهداف أداء الشركة.

ثانياً: تَرسُمُ خطةُ العملياتِ الطارئةِ (COOP) بالتفصيل كيف ستتصرَّف الشركةُ عند حدوث أي تغييرٍ في وضعيةِ الشركة التشغيلية. إنها تركِّزُ على تفاصيلِ كيفية عمل الشركة عند وقوع كارثةٍ من صنع الإنسان أو الطبيعة أو وقوع حدث إرهابي. تحدِّدُ الخطةُ مواقعَ عملٍ بديلة وبنيةً تحتيةً رديفة، وخططَ العملِ للتشغيلِ عن بعد، والمخزون المطلوب من البرمجيات والتجهيزات الخاصة بالحاسوب، واستراتيجياتِ الحصول على التجهيزات، وقوائمَ الاتصالِ مع موظفي الطوارئ، ومتطلباتِ الوصول إلى البيانات.

ثالثاً: تحدِّدُ خطةُ العودةِ إلى الوضع السويِّ من بعد الكارثة، المصادرَ التقنيةَ الهامةَ وطرقَ استعادةِ المعلوماتِ المخزنة على مثل هذه التجهيزات. إنَّها ترسمُ إستراتيجيةً تبيِّنُ المصادرَ والمراحلَ المهمة التي يجب أن تُنَفَّذَ من أجل العودة إلى الوضع الطبيعي بعد الكارثة. تُرَتَّبُ المصادرُ التقنيةُ الهامة حسبَ الأهمية وتعيَّنُ أوقاتُ الاستعادةِ المستهدفة. تُمَثِّلُ هذه المصادرُ الحاسمة المصادرَ بحدِّها الأدنى الضروريةَ لاستمرارِ عملياتِ الشركة.

يجب أن تُؤخذَ الحيطةُ عند تصميم خطّة العودة إلى الوضع السويِّ بعد الكارثة، إذ تميلُ المنظماتُ إلى ترتيب جميعِ المصادرِ على أنها مهمَّةٌ، بينما تكون في الحقيقة غير هامةٍ في المنظور الإجمالي. من الضروري تحديد فقط تلك المصادر التي يجب استعادتها من أجل استمرار العمليات.

يجب أن تُحَدَّدَ أيضاً في هذه الخطة الاتكالات المتبادلة للأنظمة الآلية، وتُقترنَ بالأولوية الحرجة المناسبة.

رابعاً: تُحَدِّدُ خطةُ أمن البنية التحتيةِ الثغراتِ والتهديدات المعروفة في البنية التحتية الموجودة للشبكة. وهذه الخطة، شأنها شأن الخطط السابقة، يجب أن تكون وثيقةً فعالةً. وعند إضافة برمجيات وتجهيزات جديدة داخل الشبكة، فإن الخطة يجب أن تعدل لتطوق أية تهديدات أو «ثغرات» جديدة. إنها تشرح بالتفصيل الاستراتيجيات التي تحد من التهديدات، وآليات الأمن داخل الشركة. كما أنها تتضمن كذلك مخزوناً بنسبة 100 بالمئة من جميع قطع التبديل التقنية، بالإضافة إلى جميع روابط الاتصالات.

تتضمنُ خطةُ تأمينِ المعلومات، على الأقل، جميعَ المصادرِ المذكورةِ سابقاً. وتبعاً لوجود متطلبات استثنائية لشركة معينة، فإنه يجب أن تُدمج خططٌ إضافيةٌ إلى خطَّةِ تأمين المعلومات. تَرسُمُ خطةُ تأمينِ المعلومات عموماً إستراتيجيةً شاملةً لحماية الشركة في كلِّ الظروفِ وتأمين استمرار عملياتها. من الضروري تحديدُ برنامج زمني لكلِّ مهمةٍ، مثل الساعة المستهدفة لاستعادة العمليات الجزئية، والمدة الزمنية اللازمة لاسترجاع جميع المقدرات التشغيلية.

يجب أن تُنشَرَ خطةُ تأمين المعلومات هذه بشكلٍ واسعٍ في أنحاء الشركة، كما ينبغي أن يُعَمَّمَ أيُّ تعديلٍ للخطَّةِ وأن تُجرى مراجعةٌ دوريةٌ لها في فتراتٍ منتظمة. إجمالاً يجب أن تجرى مراجعةٌ معتدلة سنوياً ومراجعة كاملة كل ثلاث سنوات.

يجب أن تتضمن إستراتيجيةُ تأمين معلومات إجراءَ تفتيشٍ على الأمن. وينبغي أن يَفحَصَ هذا التفتيشُ الخططَ الموثَّقةَ المذكورةَ سابقاً، وأن تُؤكِّدَ دقَّتُها وسريانُ مفعولها في البنية التحتية الموجودة. قد يتضمَّن التفتيشُ أيضاً «اختبارَ الاختراقِ» على أن تقوم به جهةٌ فاحصةٌ نزيهةٌ.

ويختلفُ غرضُ اختبار الاختراق هذا حسب حاجات الشركة. يجب أن تُحمل نتائجُ اختبار الاختراق مَحمَلَ الجدّ، كما يجب أن تنفَّذَ بدون اطلاع جميع الموظفين عليها باستثناء المدراء التنفيذيين بمن فيهم مسؤول أمن المعلومات. إن الإعلانَ المسبق لاختبار الاختراق سيؤدي إلى نتائج غير دقيقة.

يجب تَفَحُّصُ المعلومات المستنتجة من التفتيش الأمني ومن اختبار الاختراق، كما تجب المباشرةُ بوضعِ استراتيجيات الحل لتخفيف ثغرات الأمن في حال كونها ممثلة للإخفاقات الحرجة.

إجراءات الأمن الوقائية

يبدأ تطبيقُ إجراءات الأمن الوقائية بالموظفين. وكما نوقش سابقاً، يأتي التهديدُ الأعظم على أمن المعلومات من المصادر الداخلية. فتطبيق الإجراءات الوقائية على البرمجيات والتجهيزات فقط سيملك تأثيراً قليلَ الفعاليةِ في حماية البنية التحتية إذا ما وجدت تهديدات داخلية.

برامج التعليم

من المهم تعليم موظفي المنظمة وتدريبهم. إحدى طرقِ تثقيفِ الموظفين هي نموذج التعليم المرحلي. يتألف هذا النموذجُ من عدَّةِ خطواتٍ للتعليم والتدريب. تُصَمَّمُ الخطوةُ الأولى عادةً كي تُبيِّنَ المبادىءَ العامَّةَ والأهدافَ والإستراتيجية وراء أمن المعلومات. ويجب أن تتضمن هذه الخطوة التقنيات الرئيسية التي ينبغي أن يلتزم بها جميع المستخدمين، كما يجب أن تَشرح ما يترتب على عدم الالتزام بها. ويُنصَح بأن ينتهي هذا التدريب بتوقيع الموظفين على «اتفاقيات المستخدم» التي تحدد الاستخدام المسموح وغير المسموح للحاسوب والنشاطات المحظورة.

تُوضعُ الخطوةُ الثانية عادةً وفقاً للمنظور الوظيفي. يجب أن يحتوي هذا التدريب على إجراءات الأمن الإدارية والوظيفية التي ينبغي أن يتخذها الموظفون للتقليل من تهديدات الأمن.

تُصمَّمُ دوراتٌ تدريبيةٌ أخرى للمسؤولين عن أمن المعلومات في داخل كلِّ قسمٍ، ولموظفي عمليات الشبكة. يجب أن يتم تدريب موظفي عمليات الشبكة باستمرار على استراتيجيات أمن المعلومات المتطورة ضد الثغرات والتهديدات الحالية.

تعيين مسؤول الأمن

من المهمِّ تعيينُ مسؤولٍ رئيسيٍّ عن أمن المعلومات (CISO) يكون مسؤولاً عن تصميم إستراتيجية تأمين معلومات الشركة ومراقبتها. من المستحسن أن لا يكون هذا الموظف هو نفسه مسؤول إدارة المعلومات أو مسؤول المعلومات الرئيسي، لتجنب تضارب المصالح. ينبغي أن يرتبط المسؤول الرئيسي عن أمن المعلومات بالمدير التنفيذي أو المدير العام للمنظمة.

حماية موقع أنظمة الأمن

يتألف موقعُ أنظمة الأمن من عناصر البنية التحتية داخل الشركة، المحمية بواسطة آليات الأمن. تحمي هذه الآلياتُ الموقعَ من الاقتحامات الالكترونية، وأيضاً من الاقتحامات المادية من قبل الأشخاص أو الكيانات المحظورة.

قد يحمي كلٌّ من حرَّاسِ الأمن، وآليات التحكم بالأبواب مثل الأقفال، من الاقتحامات المادية، ومن الممكن كذلك الحماية من هذه الاقتحامات بوضع مراكز الحاسوب التي تخزن سجلات البيانات في مناطق لا يمكن الوصول إليها بسهولة من خلال النوافذ والأبواب.

إن استخدام مجموعة من تقنيات البرمجيات والتجهيزات قد يحمي من الاقتحامات الالكترونية. ولكن يجب أن تُرسَمَ لآليات أمن المعلومات هذه خطةٌ مفصلةٌ لتعمل بشكل فعّال. ونظراً إلى أنَّ تطبيقَ جميع أجزاء آليات الأمن هو أمرٌ مكلفٌ ومعقدٌ، فمن المستحسن تطبيق الإجراءات في تسلسل مرحلي. إن الإجراءاتِ التي تجابه أوسع نطاقٍ من الثغرات تكون عادةً أكثر الوسائل فعَّاليةً لأمن البنية التحتية. ومن الأمثلة على هذا النوعِ من الإجراءات البرامج المضادة للفيروسات وجدران النار.تُشَكِّلُ هذه الإجراءات إجمالاً الخطواتِ الأساسيةَ في بناء الموقع، فحالما يتم تطبيقها بشكلٍ فعالٍ، تُتَّخذُ خطواتٌ أخرى لتعزيز الموقع، مثل تنصيب آليات التحكم بالدخول، وأنظمة كشف الاقتحام. . . الخ. إن التفسيراتِ الموجزة المبينة أدناه تشرحُ الأجزاءَ الرئيسيةَ لموقع أمن المعلومات.

برمجيات الحماية المضادة للفيروسات

تمثل برمجياتُ الحماية المضادة للفيروس الحدَّ الأدنى في أيِّ موقعٍ لأمن المعلومات. تُنصَبُ البرمجيات المضادة للفيروس عادةً في كلِّ حاسوبٍ يستعملُ خدمةَ الإنترنت. يجب أن تبقى ملفاتُ الإرشادات حول البرمجيات المضادة للفيروس مُحدَّثةً بشكلٍ منتظم لتعمل بشكلٍ فعّال.

مخدمات إدارة البرمجيات

تُحققُ مخدماتُ إدارة البرمجيات (SMS) هدفَ تحديثِ برمجيات نظام التشغيل لدى الحواسيب التي تستعمل الإنترنت والموصولة على شبكة الشركة. يجب أن تبقى برمجيات نظام التشغيل محدَّثةً ومحيَّنةً لتَسُدّ الثغرات التي تُكتشف باستمرار من قبل المصنعين. عندما تأتي رُقَعُ التحديثِ من قبل المصنِّع، تقوم برامج (SMS) بدفع هذه التحديثات إلى كلِّ حاسوبٍ متأكدةً بذلك أنَّ النسخةَ الأخيرةَ من نظام التشغيل قد تم استخدامها.

جدران النار

إن جدرانَ النارِ (Firewalls) هي آلياتُ أمنِ معلومات تمنحُ أو تمنعُ الوصولَ إلى مواردِ المعلوماتِ الداخليةِ من قبل جهةٍ موجودةٍ خارجَ الموقع المأمون، أي من الإنترنت مثلاً. تشابه جدرانُ النارِ سلَّمَ دخولِ السفينة. يُمنَحُ الدخولُ إلى المستخدمين الذين يملكون التصريحَ اللازمَ للوصول إلى المصادر الموجودة داخل الموقع، أما المستخدمون الذين لا يملكون التصريحَ فيحرمونَ من الوصول إلى المصادر الموجودة داخل الموقع. تأتي جدرانُ النارِ على شكلين، وعادة ما يُستعملانِ معاً. إن الشكلَ الأول من جدار النار هو جهاز الكتروني، أما الشكل الآخر فهو برنامج. قد تأتي جدرانُ النار أيضاً على شكل جهازٍ لحاسوبٍ معيّنٍ. إنَّ هذا النوع من جدران النار مثاليٌ للمستخدمين الذين يعملون عن بعد خارج موقع أمن الشركة.

آليات التحكُّم بالنَّفاذ، أو الدُّخول إلى المعلومات

تَخدُمُ آلياتُ التحكم بالدخولِ هدفَ الطلب من المستخدمين تقديمَ المعلومات الثبوتية قبل أنَ يُسمحَ لهم بالوصولِ إلى مصادر المعلومات داخل موقعِ الحماية. تتألف آليةُ التحكُّم بالدخول عادةً من حاسوبِ مخدِّمٍ زاخرٍ بتطبيقات التحكم بالدخول. تكون تقنية آلية التحكُّم بالدخول غالباً غير ظاهرةٍ للمستخدمين. يُمنحُ المستخدمون عادةً حقوقَ نفاذٍ تبعاً للمجموعة الوظيفة التي يتبع لها كلٌ منهم. قد يَتَطَلَّبُ التحكمُ بالدخولِ أيضاً التوثيق أثناء كلِّ جلسةٍ، ويكون ذلك عادةً على شكل ثنائيةِ اسم المستخدمِ وكلمةِ السِّر. تَمنَحُ ثنائياتُ اسم المستخدمِ وكلمة السِّر الصحيحة الدخولَ إلى المصادرِ المطلوبة. تعد آليات التحكم بالدخول فعّالة في منع سرقة البيانات من قبل التهديدات الداخلية والخارجية.

أنظمة كشف الاختراق

إنَّ أنظمةَ كشفِ الاختراق (IDS) فعَّالةٌ إلى أبعد حد عندما تُنصَبُ بشكل صحيحٍ وتُراقبُ بانتظام. ولكن يجب الحفاظ على طريقة عمل هذه الأنظمة بسريةٍ بالغة، ومن الواجب حمايتها بثقة شديدة. تُسَجِّلُ أغلبُ أنظمة الكشف (IDS) جميعَ التعاملات التي تجري داخل موقع الحماية وجميع الطلبات التي

تأتي من خارجه. يؤدي تحليلُ المعلومات في سجلات الأحداث إلى تحديد المتناقضات و/أو النشاطات والإجراءات غير النظامية. وعادةً ما يُفرَضُ تَفَحُّصٌ إضافيٌ على التعاملاتِ الجاريةِ على الشبكة من خارج موقع الحماية. إن أنظمةَ كشف الاختراق فعّالة في منع سرقة البيانات من قبل التهديدات الداخلية والخارجية.

آليات التعمية (التشفير)

تَصلُحُ التعميةُ في حماية البيانات أثناء عملية الإرسال. يجب أن تُنصَب تطبيقات التعميةِ على كلٍّ مِنَ الحاسوبِ المرسلِ والمستقبلِ. يقوم الحاسوبُ المرسلُ أثناء عملية إرسال البيانات بتعميةِ البياناتِ قبل الإرسال. فور استلام البيانات المعماة يقوم الحاسوبُ المستقبلُ بفكِّ التعمية عن البيانات. إن خوارزمياتِ التعميةِ المباعةِ من قبل العديد من الشركات هي أساس آليات التعمية. وكلما كانت الخوارزمية معقدة، كانت عملية إرسال البيانات أكثر أمناً، إلا أنَّ أداءَ الحاسوبِ وسرعةَ عملهِ يتراجعان مع الازدياد في التعقيد الخوارزمي. إن تقنيات التعمية فعَّالةٌ ضد اكتشاف الرسائل خارج موقع الحماية.

وسائل قطع اتصال الشبكة

إن وسائلَ قطعِ اتصال الشبكةِ هي آلياتٌ تقومُ حالاً عند الضرورة بقطع الاتصالات السلكيةِ واللاسلكية بين موقع الحماية والمحيط الخارجي، فعند حدوث اختراق ما، أو هجمة الحرمان من الخدمة، تُقطعُ قنوات الاتصالات السلكية واللاسلكية فوراً بدون التسبب بضرر خطير لأنظمة الشبكة داخل الموقع. تقوم وسائلُ قطع اتصال الشبكة بالعمل نفسه الذي تقوم به الإزالة المادية لمقبس الاتصالات السلكية واللاسلكية أو مزود الكهرباء الذي يفصل الكهرباء عن جهاز الحاسوب بدون التسبب بضرر خطير أو فقدان للبيانات. تتألف وسائل قطع اتصال الشبكة عادةً من البرمجيات والتجهيزات في وحدة مفردة. يُفعَّلُ عادةً ضبط أمر قطع الاتصال يدوياً أو بوساطة إشارات الخطر من قبل أنظمة كشف الاختراق. عندما يُقطَعُ اتصالُ موقعِ الحمايةِ، لا تستطيع المنظمة الاتصال خارج الموقع، ولكنها تستطيع تمكينَ المختصين بالأمن من

تشخيص، وربما إصلاح، الثغرات لتحمي من التهديد قبل إعادة وصل قنوات الاتصالات السلكية واللاسلكية.

استنتاجات

إن حمايةَ المعلومات الخاصَّة بالزبون هو عملٌ معقدٌ ومليءٌ بالتحدي. على أية حال يجب أن تقوم المنظمات بتأمين السِّرية لزبائنها إذا ما أرادت أن تحيا في السوق الالكترونية العالمية. ليس على المنظمات مطلباً قانونياً لتحقيق أمن المعلومات فحسب، وإنما تحمل كذلك مسؤوليةً حرفيةً تجاه شركائها في العمل على طول سلسلة التزويد.

إن أمنَ المعلومات لعبةٌ خاسرةٌ، إذا استعملنا الإجراءات التقليدية فقط، ولكن التطبيق الفعَّال لهذا الأمن سيسفر عن نجاحٍ وجزاءٍ طويل الأمد.

على الرغم من أن أمنَ المعلومات لعبةٌ ديناميكيةٌ متطورةٌ باستمرار، إلا أن المنظمات تستطيع اتخاذ قرارات صحيحة إذا ما طبَّقَت استراتيجياتٍ شاملة ومفصلة لتأمين المعلومات، كي تحتفظ بمكانتها في السوق مع الحماية أيضاً من التهديدات.

الفصل الرابع

استراتيجيات شاملة لإدارة المخاطر المحدقة بتقنية المعلومات

كريسان هيرود

جامعة الدفاع الوطني، الولايات المتحدة الأمريكية

المقدمة

يشرحُ هذا الفصلُ السببَ وراء أهمية أن تُطوِّرَ المنظمات وتُنشِىءَ وظيفة إدارة مخاطر تقنية المعلومات، وأن تَستَخدِمَ أفضلَ الممارسات لتقييم أثر المخاطر، وخاصة تلك الممارسات التي تعدُّ المعيار الشائع لقياس وتقييم أثر المخاطر داخل المنظمات. إن إدارةَ مخاطر تقنية المعلومات وظيفةٌ جديدةٌ هامةٌ قد تساعد الشركات على تحقيق خدمة تقنية معلومات ذات مستوى عالمي.

تتضمنُ إدارةُ مخاطر تقنية المعلومات الالتزامَ بالأنظمة، وأمنَ المعلومات، والعودةَ إلى الوضع السوي بعد الكارثة، ومخاطرَ المشروع. يجب أن تكون إدارةُ مخاطر تقنية المعلومات جزءاً من إستراتيجيةِ الشركة في إدارة المخاطر، كما هو الوضع مع إدارة المخاطر المالية وإدارة مخاطر السمعة. ونظراً إلى تزايدِ تعقيد البنى التحتية لتقنية المعلومات، ونظراً إلى استمرار الشركات بالاعتماد

على الإنترنت كأساسٍ للاتصال في تعاملاتها التجارية الالكترونية، فإن المخاطر المرافقة في ازدياد. لهذه الأسباب فإن اختيارَ سيرورةٍ لإدارة المخاطر ثم تطبيقها واختيار طريقةٍ معياريةٍ لذلك، سوف يقلّل إلى حدٍ كبيرٍ من المخاطرِ المتعلقةِ بإدخالِ تقنياتٍ جديدة تدعم مهمة الشركة.

إن التعقيداتِ المتأصلةِ في تطوير خدمات تقنية المعلومات وإدارتها ونشرها على المستوى العالمي واضحة. أضف إلى هذه التعقيدات الإطارَ التشريعي والتنظيمي الذي يتحكَّمُ بممارسات الشركة في العديد من الصناعات، وعليه تواجه الشركاتُ وضعاً يتطلَّبُ التيقُّظَ الدائمَ لضمانِ عملها بأمانٍ وشرعيةٍ. لا يمكن إزالة المخاطر من دورة حياة الشركة، وتؤدي الإخفاقات إلى خسارةٍ وأضرارٍ وادعاءات قضائية. بنفس الوقت فإن تقنيةَ المعلوماتِ عنصرٌ جوهريٌ في نجاح أيِّ شركةٍ، إذ إن استغلالَ تقنيات المعلومات يخلقُ العديد من الفرصِ لتَطَوُّرِ الشركةِ ولِخِدمَةِ الزبائن.

من المهم أن تَهدفُ وحدة إدارةِ مخاطرِ تقنيةِ المعلوماتِ إلى ضمان أن المخاطر المحتملة قد حددت وقيِّمَ أثرها، وإلى تطبيق الضوابط التي تخفف الأثر المحتمل للمخاطر أينما تجد الشركة ذلك ضرورياً.

يُحَقَّقُ هذا بوساطة ما يلي:

- رسم **سياسة**.
- إجراء تحسينات **للعمليات**.
- تحديد **إجراءات أو معايير**.
- تأسيس إجراءات تحكمٍ من خلال **ممارسات الإدارة**.
- إتباع **الإرشادات**.
- إبرام **العقود**.
- الاستعانة بجماعات في **المنظمة**.
- **الاستعانة بجهات خارجية أو التعهيد الخارجي** عند الضرورة.
- **التأمين** ضد الحوادث.

تعريف إدارة المخاطر

إن الخطرَ هو حدثٌ أو ظرفٌ غير مؤكد الحدوثِ، والذي إذا ما حدث فقد يؤثِّرُ سلباً في النشاطات المنجزةِ في الشركة. إدارة المخاطر عمليةٌ منتظمةٌ: لتحديد المخاطر، وتقدير احتمال ظهورها، والأثر الذي قد تتركه، واتخاذ الإجراء الضروري لضمان الحصول على ثمرة النشاطات المنجزة.

إن إدارةَ المخاطر هي موازنةُ المخاطر مقابل الثمرة، وذلك لضمان أن الثمرات تزداد إلى أقصى حدّ، وأن المخاطر تتناقص إلى الحدّ الأدنى لتصل إلى درجة مقبولة للشركة.

مفتاح النجاح في إدارة المخاطر

إن مفتاحَ إدارة المخاطر هو تحديد المخاطر وإداراتها بحيث تتجاوز الثمرةُ المرجوَّةُ أثرَ المخاطرِ المواجهة. هذه المهمةُ مستحيلةٌ ما لم تُحَدَّد المخاطر، فالمخاطر التي لا تُحَدَّد ولا تعالج جيداً قد تسبّب ضرراً عظيماً.

إدراك القوى المحركة للمخاطر

كلما أحدثت الشركة تغييراً ما، فإنها تُحدثُ أيضاً قوى محركةً تؤثِّرُ في المخاطر. يسبب التغييرُ زيادةً أو إنقاصاً في المخاطر. للتغيير غالباً ثمرةٌ وفائدةٌ مرافقةٌ، الأمر الذي يجعلُ الشركةَ مستعدةٌ لمواجهة المخاطر التي قد تنجمُ عن هذا التغير.

تبدأ إدارةُ المخاطر بمراقبة البرامج والمشاريع والعوامل الداخلية والخارجية الأخرى التي قد تُحدثُ مخاطر. سوف يولد التغييرُ في الشركة غالباً مخاطر متعددةً محتملةً. وقد يؤثر كلُّ خطرٍ منها في العديد من وحدات الشركة أو مجالاتها الوظيفية.

الاستجابة للمخاطر

تشتمل الاستجابةُ للمخاطر، أو التعامل معها، واحدةً من القرارات الآتية:

1. تخفيف المخاطر: حيث تُتَّخَذُ الخطوات للتقليل من احتمال نضوج الخطر (حدوثه)، أو لتقليل الأثر أو الخسارة إذا كان لا بد من ظهور ذلك الخطر.

2. تجنّب المخاطر: حيث يُتَّخَذُ القرارُ بتجنب التعرض للمخاطر أصلاً، وهذا يعني إجمالاً أن الثمرة/الفائدة لن تكتسب للشركة.

3. نقل المخاطر: حيث تُنقل الخسارة المتوقعة نتيجة لوقوع الخطر إلى طرف آخر. ويكون هذا الطرف عادةً الفريق الثالث (على سبيل المثال التأمين ضدَّ الادعاء القضائي).

4. قبول المخاطر: حيث لا تُتَّخَذ الخطوات من أجل تخفيف، أو تجنب أو نقل الخطر. تختار الشركة في هذا القرار عادةً تَقَبُّلَ تبعات حدوث الحظر إذا كان لا بد منه.

إطار عمل إدارة المخاطر

من المهم أن يُبنى قرار الاستجابة للمخاطر على استخدام إطار عملٍ أو منهجيةٍ معياريةٍ لإدارة المخاطر. كما ينبغي أن لا تتّخذ القراراتُ حول طريقة إدارة المخاطر بمعزلٍ عن الآخرين، وبالتأكيد يجب أن لا تتخذ بدون الحذر المطلوب. يُقَدِّمُ إطارُ عملِ إدارةِ المخاطر العمليةَ التي إذا ما جرى اتّباعها فإنها ستؤدي إلى قاعدةٍ منطقيةٍ لاتخاذ القرارات، وعندها تُجمَعُ الحقائق والبيانات وتُطرَحُ بطريقة عقلانية.

ثمة العديد من الطرقِ المتَّبعةِ لإدارةِ المخاطر في كلٍّ من القطاع العام والخاص. لا توجد طريقة أفضل من الأخرى، فأطرُ العملِ، ومنها المطروح في هذا الفصل، يجب أن تُنَقَّحَ لتلائم محيط و/أو ثقافة الشركة. إجمالاً هناك أشياءُ رئيسيةٌ وجوهريةٌ تقودُ إطارَ عملِ إدارةِ المخاطر هي:

- يجب النظر إلى المخاطر وإلى تأثيرها بشكلٍ شمولي ـ أي من منظور الشركة بأكملها، فتقدير تأثير المخاطر من منظورٍ أضيق يثير أخطاراً بحد ذاته باعتبار أن حاجات الشركة قد تفوق أهميةً التأثير السلبي لتقنية المعلومات.

- إن المخاطرَ لا تكون جسيمةً إلا إذا كان لها تأثيرٌ محددٌ في الشركة أو خسارةٌ قابلةٌ للقياس.

- يجب أن يقدم إطارُ العملِ قاعدة تسمحُ بتخمينِ جميع أنواع المخاطر، ابتداءً من حوادث الأمن الثانوية وانتهاءً بالحوادث الفاجعة.

● قد يكون ضرورياً أحياناً أن يجري التعاملُ مع الأحداث قبل دراسة الباعث الذي سبّب ظهورها ـ إن معاملةَ المخاطر بصورةٍ شموليةٍ لا تعني أن ندع الشركة تنهار قبل تصحيح المشكلة.

قابلية التوسع في عمليات إدارة المخاطر

يقتضي تناولُ إدارةِ المخاطرِ اتِّباع منهجٍ قابلٍ للتوسعِ أو التعميمِ ليتعامل مع مصادر وأحجام مختلفة للمخاطر. قد يتضمن هذا عادةً استخدامَ إطَار عملٍ لإدارة المخاطر وفق طرقٍ متعددةٍ، بادئاً ربما من نقاط انطلاقٍ مختلفةٍ.

يجب أن تتعامل قابلية التوسُّعِ أو التعميم مع كلٍّ من مصادرِ الخطرِ التالية:

● مخاطر الشركة الرئيسية: مثل الاندماج، أو الاستحواذ، أو استحداث فرص ومواقع تجارة الكترونية جديدة، أو القوانين والقضايا القانونية.

● مخاطر تقنية المعلومات الجوهرية: مثل استحداث تقنيات جديدة داعمة لعمليات الشركة سواء أكانت داخلية أو خارجية.

● مخاطر المشروع:

1. مخاطر على استمرارية الشركة قد يسبّبها المشروع.
2. مخاطر حول أرباح المشروع (المخاطر على تحقيق فوائد المشروع).
3. مخاطر التسليم الناجح للمشروع.

● الحوادث والمخاطر القائمة بذاتها: وهي متأصلة في العمل والممارسات التي تتضمن استخدام وتطبيق تقنية المعلومات.

إدارة المخاطر هي مسؤولية كل شخص

نظراً إلى أن المخاطرَ موجودةٌ حكماً في كلِّ أمرٍ تقوم الشركة به، فإن إدارةَ المخاطر جزءٌ من عملِ كلّ شخص من أجل تحقيق أهداف الشركة كاملةً. من المهم أن تُقَلَّلَ التهديداتُ التي تجابه أهداف الشركة لتصل، على الأقل، إلى الحدِّ الذي تفوقُ به الثمراتُ المرجوةُ أثرَ التهديدات المحتملة.

ولكي تتأكد من أن إدارةَ المخاطر تعملُ كما يجب، قم بطرح الأسئلة التالية:

- ➢ هل أنت على دراية بعمليات الشركة التي تدعم العمل اليومي؟ وهل تعلم ما هي الفائدة المرافقة للأعمال اليومية الناجمة عن تلكم العمليات؟
- ➢ هل تدرك أيّاً من ضوابط تقنية المعلومات (السياسات، والعمليات، والممارسات، وإجراءات العمل القياسية (SOPs)/ المعايير) ترتبط بعملك؟ هل تستجيب لهذه الضوابط؟ هل تطبق هذه الضوابط بشكل كامل داخل نطاقك؟
- ➢ هل تحدد المخاطر المتأصلة وتديرها في مشاريعك وفي مخرجاتها؟
- ➢ هل تبحث بشكل واع في المخاطر المتعلقة بعملك وتديرها، وكذلك في كيفية تأثيرها في نطاقك أو في نطاقات الشركة الأخرى؟

سرية وثائق إدارة المخاطر

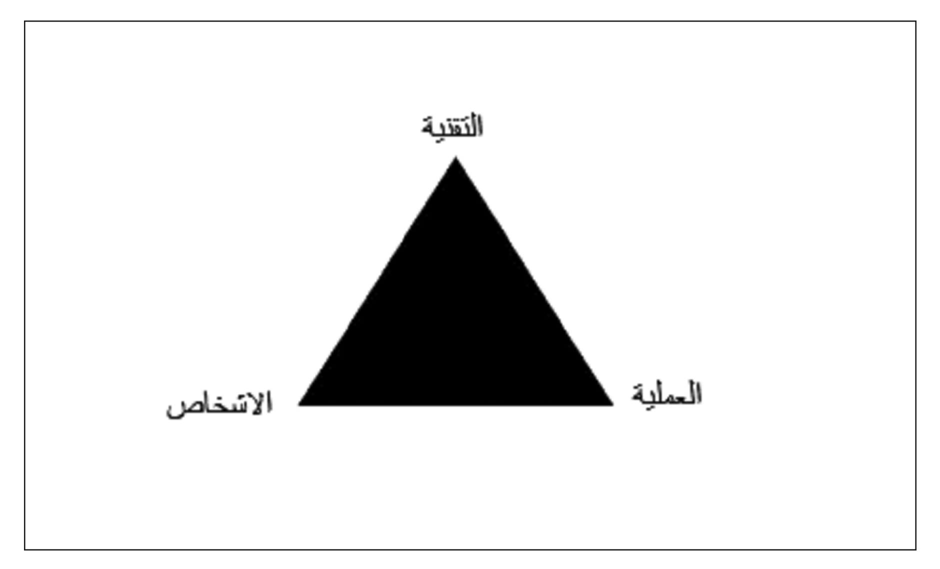
تحتوي غالباً الوثائقُ المتعلقة بعمليةِ إدارة المخاطر على معلوماتٍ سِّريةٍ للغاية، لذلك يتوجب حمايتها. إن هذه الوثائق قد تحتوي كذلك على معلوماتٍ لها تأثيرات تنظيمية وقانونية محتملة في الشركة. ينبغي التفكير، في بداية كل مشروع وقبل صياغة أي وثائق، فيما إذا كان هذا المشروع يتضمن مثل هذه الآثار، فإذا كان كذلك فمن الضروري توظيف موظفين مناسبين من جهاتٍ أخرى يعنيها ذلك في المنظمة.

الأشخاص والعمليات والتقنية والتسلسل الهرمي للضوابط

إن إدارة المخاطر هي عمليةُ تخفيف الخطر أولاً وقبل كل شيء. وقد ينفَّذُ هذا بوساطة تقليل الأثر و/أو بوساطة تقليل احتمال حدوث هذه المخاطر. تطبق لتحقيق ذلك «ضوابط» متنوعة وفق تسلسلٍ هرمي محددٍ لهذه الضوابط. ويحدد هذا التسلسل الهرمي للضوابط المصطلحات الفنية المستخدمة لوصف إدارة المخاطر. يعتمد نجاح إدارة المخاطر على قدرتها في إدخال التغيرات في تقنيات المعلومات في مجالات: السياسة، والعملية، والممارسات الإدارية، والإجراءات والمعايير. من الضروري للقيام بذلك أن يسود كلَّ أنحاء الشركة تفهمٌ عامٌ حول استخدام هذه المصطلحات.

توجد ثلاثة عناصر جوهرية تتعلق بتخفيف المخاطر (الشكل 1). إذ قد يظهر التغيير في الأشخاص، أو في العمليات أو في التقنية:

➢ **الأشخاص**: من الممكن تغيير الأشخاص، أو بدقة أكبر تغيير أفعالهم، من أجل تخفيف المخاطر. وكمثالٍ على ذلك القيامُ باعتماد ممارسات حيال ترخيص البرمجيات، بحيث تُفَصَّلُ المتطلبات الواجب التقيد بها عند شراء البرمجيات وتوزيعها. من المهم أن يكون الموظفون على درايةٍ بالإجراءات المناسبة المتعلقة بشراء البرمجيات، كما ينبغي أن يعلموا أن تحميل البرمجيات من الإنترنت هو إجراءٌ غير مسموحٍ به.



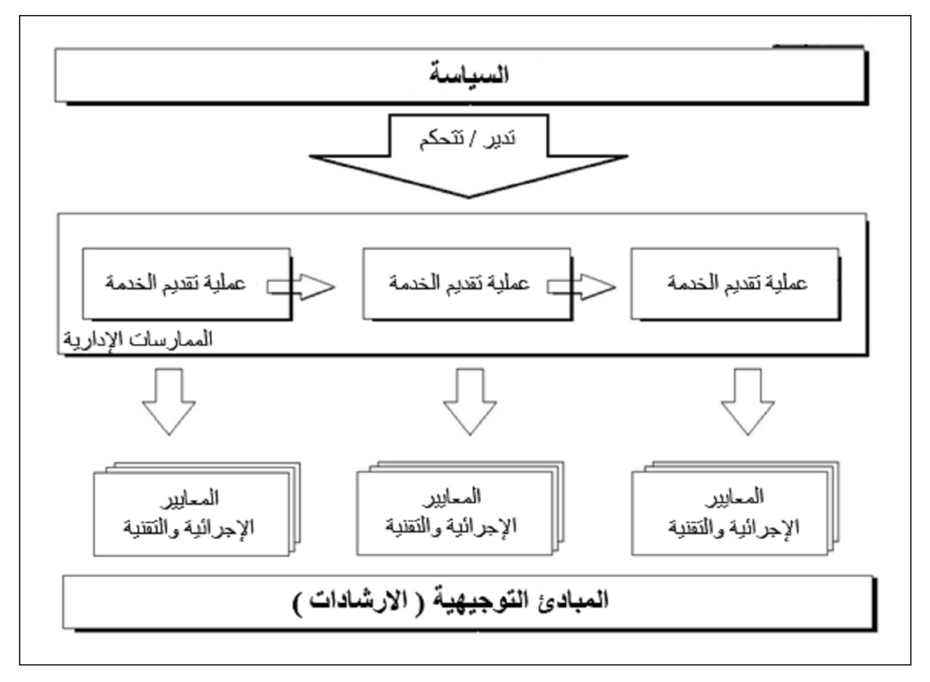
الشكل (1).

➢ **العمليات**: قد تُغيَّرُ العمليات لتخفيف المخاطر. سيكون المثال على ذلك إدخال عمليات إدارة النفاذ (والبرمجيات المرافقة) لتقليل المخاطر التي تنتج من عدم إدارة هذا النفاذ، مثل إيقاف النفاذ إلى معلومات الشركة من قبل الموظف فور تركه العمل.

➢ **التقنية**: من الممكن إدخال التقنية أو تعديلها لضمان تخفيف المخاطر. والمثال على ذلك هو أدوات برمجيات المراقبة والتفتيش على الأنظمة والتطبيقات الحساسة لمنع النفاذ المحظور.

التسلسل الهرمي للضوابط

توصفُ الضوابطُ عادةً على أنها وثائق تُعزِّزُ التغيير، وتنعكسُ في كثيرٍ من الأحيانِ في وثائقِ السياسية، ويشار إليها كذلك بالتسلسل الهرمي للضوابط. إن امتلاك نموذجٍ للضوابط يشكِّلُ إطار عملٍ من أجل تخفيف المخاطر، وذلك من خلال تحديدٍ الأفعال أو المخرجات التيِ من شأنها، إذا ما نفذت، أن تقلل من المخاطر. يقوم الشكل (2) بشرحِ مثالٍ للتسلسل الهرمي للضوابط.



الشكل (2).

المصطلحات الفنية الشائعة

تصف المصطلحات الفنية التالية الضوابط المختلفة المستخدمة لتخفيف المخاطر:

➢ **السياسة**: تدير السياساتُ ممارساتِ العملِ الموثوقة والآمنةِ لضمان إجراء العمليات على نحوٍ يقلّل المخاطر المحدقة بالشركة. وتعدُّ السياساتُ بمثابة عقدٍ بين رب العمل والموظفين كما أنها ملزمة.

➢ **العملية**: إن العمليةَ هي «الأمرُ الذي نقومُ به» وتشرح بوضوحٍ الخدمةَ والمُخرَجَ المستهدف. ومن الممكن وصف العملية في مستوياتٍ عديدة.

➢ **المعيار الإجرائي**: يشرح بالتفصيلِ كيف يجب أن يؤدى العمل. قد توضع هذه المعايير الإجرائية من قبل إدارة تقنية المعلومات لاستخدامها الخاص، أو قد تُفرض على مستوى المؤسسة ككل.

➢ **المعيار التقني**: يحدد الأدواتِ أو القواعدَ الموضوعة كي تستخدم في تنفيذ العملية أو الإجراء. من الممكن أن يكون مصدر المعيار داخلياً أو خارجياً. سيتم اعتبار الحلول التقنية على أنها معايير تقنية في التسلسل الهرمي للضوابط.

➢ **الإرشاد**: يقوم بوصف الممارسات المثلى لإنجاز العملية. إن هذه الممارسات ليست إلزامية على خلاف إجراءات العمل القياسية (SOP) أو المعيار التقني.

➢ **عملية إدارة المخاطر**:

■ **تقييم أثر المخاطر**: تحديدُ المخاطر التي حدثت نتيجة للتغير في الشركة وتعيين أثرها، وتقرير ما إذا كان الأمر يقتضي اتخاذ الخطوات لإدارتها.

■ **تخفيف المخاطر**: تصميمُ وتنفيذ الضوابط الضرورية لتخفيض أثر المخاطر المحتمل إلى مستوى مقبول.

نموذج إدارة المخاطر

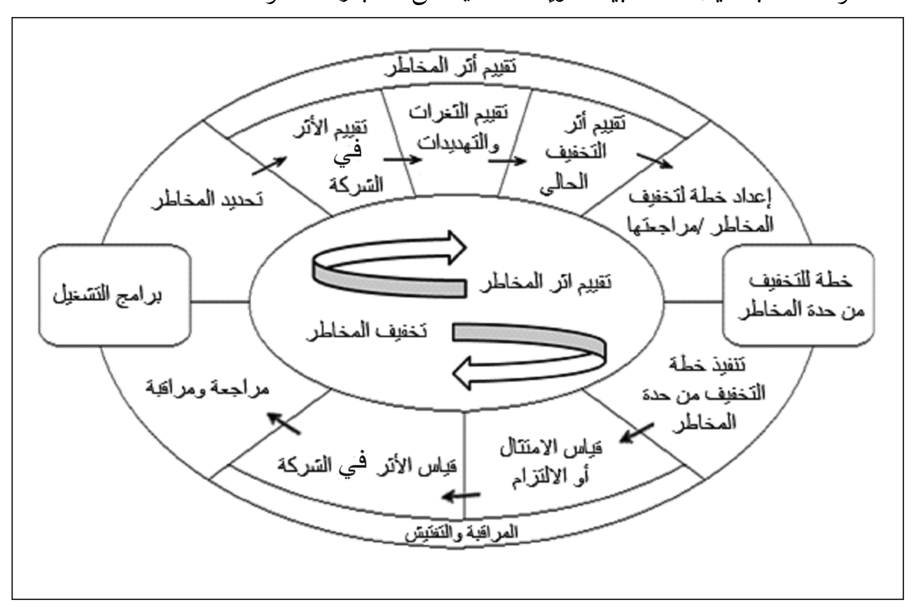
لكي يُقَيَّمَ أثرُ المخاطرِ ويُخَفَّف، يجب استخدام طريقة معيارية. كما ذُكِرَ سابقاً في هذا الفصل، لا توجد طريقةٌ لإدارة المخاطر أفضل من الأخرى. إن الطريقةَ المشار إليها في ما يلي هي مجموعة من أفضل الممارسات من نماذج حكوميةٍ وصناعية، وأكثر ما يستحق الذكر منها هو «المعهد الوطني للمعايير» الأمريكي NIS، وجمعية ضبط الرقابة على التقنية وأنظمة المعلومات الأمريكية TISACA، ومعيار منظمة أيزو العالمية (ISO 17799).

ليس النموذج هو مفتاح النجاح، وإنما كون النموذج مناسباً لشركتك،

وكونك، أنت، كمدير لمخاطر تقنية المعلومات، قادراً على تحقيق المكاسب للشركة من امتلاك طريقة لإدارة المخاطر. إن اعتمادَ طريقةٍ معياريةٍ، تستخدم من قبل جميع وحدات الشركة لتقييم أثر المخاطر، هو عماد البرنامج الناجح. تناقشُ الفقراتُ الآتية نموذج إدارة المخاطر، كما هو مبّين في الشكل (3)، وتحدِّدُ خطواتِ العملية ونشرها.

مقدمة في أهمِّ المصطلحات

المخاطر: إن الخطر هو وضعٌ أو نتيجةٌ سيسفرُ عنها أثرٌ سلبي. يقترنُ الخطرُ دائماً بالنتيجة السلبية، وإلا فلا يمكن اعتباره خطراً.



الشكل (3).

مصدر المخاطر: إن مصدر المخاطر هو حدثٌ أو ظرفٌ يؤدي إلى ظهورِ الخطر، أو تغييرِ أثره المحتمل، أو تبديلِ احتمال ظهوره.

التهديد: هو الإمكانية أو القدرة على التسبب بالضرر. إنه الشخص أو الشيء الذي سيسبب أثراً مالياً إذا ما وقع الخطر.

الثغرة: إن الثغرةَ شيءٌ متأصلٌ، أو مُتضمَّنٌ حكماً في الحالة التي توجد فيها مخاطر، وتُحدثُ الثغرةُ ضعفاً (أي: وضعٌ موجودٌ حكماً، شئنا أم أبينا،

يحتوي على نقطة ضعفٍ تجعلنا عرضةً لشيء ما). تمتلك الثغرةُ القدرةَ على زيادة احتمال وقوع الخطر أو زيادة احتمال الخسارة أو أثر وقوع الخطر.

الثمرة: هي النتيجةُ الايجابيةُ التي قد تُحرز/ تُحقق إذا ما عرَّضنا أنفسَنا للمخاطرِ. إن الثمرةَ تجعل عملية التعرض للمخاطر جديرةٌ بالاهتمام، وتكون الثمرةُ عادةً المكافأة الموعودة التي تُسوِّغ مجابهة الخطر. قد تؤدي المخاطرةُ إلى ثمرةٍ مضمونةٍ وقد لا تؤدي. قد تعرِّضُ المخاطرُ الثمرة/ الفائدة للفقدان.

الاستجابة للتخفيف: هي مجابهة المخاطر باتخاذ التدابير للتقليل من أثرها.

مفاهيم نموذج عملية إدارة المخاطر

إن بعضاً من المفاهيم الجوهرية المُتَضَّمَنةِ في نموذج عملية إدارة المخاطر جديرةٌ بالاهتمام:

- نادراً ما يتم التخلص من المخاطر كلياً، فهي تُخَفَّفُ فقط أو يُسيطرُ عليها، ولذلك فإن نموذجَ إدارةِ المخاطر هو حلقةٌ دوّارةٌ لا نهاية لها. بعد أن يتم تقليل الخطر يجب تفحصه دورياً، كما ينبغي أن توضعَ الضوابط تحت الاختبار على فترات منتظمة للتأكد من حسن الالتزام بها.
- إن خُطوَتَي العملية الجوهريتين، أي تقييم أثر المخاطر وتخفيف المخاطر، تجمعان على التوالي المعلومات التي تدعم الخطوات الأساسية في مجمل العملية.

تحديد المخاطر

إن الخطوةَ الأولى لعملية تقييم أثر المخاطر هي المراقبةُ المستمرةُ المطلوبةُ لاكتشاف التغيرات في بيئة الشركة، لا سيما القوى المحركة التي قد تؤدي إلى مخاطر إضافية أو تعديل تلك الموجودة في الشركة. إن من الخطوات الرئيسية في أيَّةِ تقنية لإدارة المخاطر خطوة تحديد منظور المصالح، (أي من وجهة نظر من يجب أن يحلل مشهد (سيناريو) المخاطر)، أو من الذي سيتكبَّد عملياً خسائر، ومن سيكتسب ثمرات؟

من أجل الوصول إلى منظور متكامل للشركة، قد يكون من الأهمية بمكان، فيما يتعلق ببعض مشاهد المخاطر، تحليل الوضع نفسه من أكثر من منظور (على سبيل المثال: قد يكون لدى كل من وحدات الشركة المختلفة، أو المجالات الوظيفية داخل الشركة، وجهة نظر مغايرة حيال خطر ما).

تحديد نطاق العمل

يُعدّ تحديدُ مجال العمل محوراً هاماً آخر لإدارة المخاطر. ينبغي عند إدارةِ عملية تحديد الخطر الاتفاق على فهمٍ واضحٍ لحدود التحليل وعلى المواضيع التي يشملها التحليل. ما هو الشيء المَشمولُ وما هو الشيء المستبعد؟ إن هذا ضروريٌ، خصوصاً عند حساب كمية الخسارة أو الفائدة/ الثمرة اللتين تتأثران بشكل مباشر بكمية وحجم مواضيع المجال.

قد يشتمل مجالُ العملِ على التقنية، والحدود التنظيمية، والجغرافية والوظيفية.

من الضروري جداً تحديدُ مجال العمل بغيةَ تحليلِ مواقع الخطر الرئيسية، وذلك كي نتعامل مع مقادير من المعلومات سهلة السيطرة (فقد لا يكون ممكناً جمع البيانات حول كامل الأثر لقانون تنظيمي جديد في جلسة واحدة من جلسات تحديد المخاطر ـ فقد يكون المجال واسعاً جداً وعندها يكون تقسيم المجال ضرورياً). وعادةً ما يتغير ممثلو الجهات ذات المصلحة مع تغير نطاق عمل تقييم أثر المخاطر.

من الأقوال التي تُعَرِّف نطاق العمل في تحديد المخاطر ما يلي:

- يتضمن هذا النطاق جميعَ أنظمة تقنية المعلومات في المؤسسة، سواءٌ كانت داخلية في الشركة أو التي تدار خارجياً بواسطة المزودين، ولكنها تستبعد جهاز قيادة العمليات وأنظمة الحاسوب.
- جميع أنظمة الحاسوب من أيِّ نوعٍ كان، وتقنية المعلومات، وجهاز قيادة العمليات.
- جميع أنظمة حواسيب تقنية المعلومات الخاضعة لقواعد خاصة، على سبيل المثال: في الشركات المالية والمستحضرات الصيدلية.

قياس الثمرة المحتملة

تجني كلُّ قوة محركة جديدة أو معدلة ثمرةً مقابلةً. قد تتضمن هذه الثمرة:

1. مجموع المبيعات أو الربح المتوقع.
2. التخفيض في الخسارة المتوقعة.
3. عوائد التعاون: توفير ناتج من تكاتف الجهود.
4. تجنّب تكلفة أو توفير في التشغيل.
5. تجنّب خسائر فقدان السمعة.
6. القدرة على الاستمرار بممارسات الشركة الموجودة رغم التغيرات في الظروف الخارجية.

من المهم الأخذ بعين الاعتبار كلاًّ من **وصف** الثمرة و**قيمتها** المحتملة معاً.

قياس المخاطر

لتقرير ما إذا كنت ستتوصَّل إلى إنجازِ عمليةٍ كاملةٍ لتقييم أثر المخاطر، لابد من إلقاء نظرةٍ شاملةٍ على القوَّةِ المحركةِ وراءَ التغيراتِ الجديدةِ أو المعدلة، وتتضمن المجالات التي تتطلب البحث:

- السبب الذي أدى إلى التغيير.
- النتيجة المحتملة.
- مُبرِّراتُ التغيير والمنطق وراءه.
- من الذي أحدثَ التغيير.

قم بتحديد المخاطر المحتملة المحدقة بالشركة انطلاقاً من فهم التغيير في القوى المحركة. قد تكون هذه المخاطر أخطاراً سابقةً قد تمّت دراستها من قبل، أو قد تكون أخطاراً جديدةً. لخِّص مخاطر الشركة في كلٍّ من الأعمال التجارية للشركة، ، وتقنية المعلومات، كلاًّ على حدة.

عند الانتهاء من تحديد المخاطر، يجب إجراءُ مراجعةٍ لتعيين المخاطر التي جرت معالجتها ووضعت لها ضوابط من خلال جهودٍ سابقةٍ، والمخاطر الجديدة التي لم يتم تفحصها رسمياً في الماضي.

فيما يتعلق بكلّ خطرٍ جرى تحديده، قم بالبحث في **وصف** الخطر و**التكلفة** المحتملة له. إذا كان الخطر قد تمّ تحليله سابقاً، فقم بتلخيص **نتائج الفحص السابق**.

الأثر في أعمال الشركة

تتضمن الخطوةُ الرئيسيةُ التالية تحديدَ أثر المخاطر في الشركة. تشتمل هذه الخطوةُ على تحليلٍ مفصلٍ لجميعِ المخاطرِ التي جرى تحديدها. إن الهدفَ هو تقديرُ الأرجحيةِ والأثرِ المحتملِ لهذه المخاطر من أجل اتخاذ قراراتٍ واعيةٍ حول الخطوات المناسبة التالية.

تحليل المخاطر

يجب أن تُحلَّل كلُّ المخاطر وتُصنَّفَ إلى فئاتٍ حسب تأثيرها في أنشطة الشركة، إن القائمة البسيطة لذلك هي:

- أمان تطوير المنتج.
- جودة المنتج وتوفره.
- نظم تقنية المعلومات.
- إدارة المعلومات.
- الحفاظ على الأصول، والموارد والمعلومات الأساسية
- ممارسات التسويق والمبيعات.
- نزاهة المدراء والموظفين.
- عدم التمييز في التوظيف.
- معاشات التقاعد.
- الضوابط المالية.

- قانون التنافس.
- الإدارة البيئية.
- سلامة الموظف وصحته.
- المقاضاة.

قس المستوى الحالي للمخاطر.

نبيّن فيما يلي طريقةً نموذجيةً لقياس المخاطر. إن معيار القياس هذا يرتكز على اعتبارين اثنين هما:

1. القيمة المتوقعة أو الأثر المالي، ونرمز له بـ (الأثر المالي $)، إذا ما وقعت المخاطر يجب تفحص ذلك دائماً من وجهة النظر التجارية، وليس من منظور التقنية.

2. إحتمال أو أرجحية وقوع الخطر ونرمز لها بـ (إ).

وتكون صيغة أو معادلة أو قانون حساب المخاطر هي:

قيمة الخطر($) = الاحتمال (إ) × الأثر المالي ($)

يتطلب قياسُ المخاطر معرفةَ القيمة المتوقعة لأثرها في أعمال الشركة إذا ما وقع الحدث. يجب أن تَحسُبَ وحدات الشركةِ المتأثرةِ هذا الأثرَ المالي.

تُعَرَّفُ القيمةُ المقبولةُ للقياس المتعلقِ بكلِّ خطرٍ من المخاطرِ بـ **المستهدف**. وإذا ما اعتمدنا مستويات معيارية لقيمة هذا **المستهدف**، فإن ذلك سيزودنا بطريقة لقياس مدى جودة إدارة المخاطر أو تخفيفها عندما نقوم بإدارة المخاطر وفق إطار العمل.

عندما نحسب مستوى قيمة المستهدف لخطر من المخاطر، يجب استعمال صيغة أو معادلة أو قانون حساب الثمرة (ما هو مستوى الخطر المقبول الذي تستطيع الشركة الموافقة عليه مقابل ما تجنيه من الثمرة المرافقة). هذا هو مستوى المستهدف، إذا كان مستوى الخطر الحالي يعادل هذا المستهدف، عندئذ لن يكون التخفيف مطلوباً وستقبل الشركة هذا الخطر.

تقييم أثر وجود الثغرات

يحدِّدُ هذا التقييمُ جميعَ المقومات التي قد تساهم في وقوع الخطر المحتمل. يشار إلى هذه المقومات بـ **الثغرات والتهديدات**. في معظم الحالات، سيكون هناك العديد من الثغرات والتهديدات لكل المخاطر المحتملة على الشركة.

لا تنهمك كثيراً في المناقشةِ التي تدورُ حول تعاريف التهديدات والثغرات، فهذا لا يهم طالما أن شركتك تمتلك فهماً عاماً لهذين المصطلحين، إن المناقشات المبالغ فيها حول المصطلحات تعرقل العمليات.

حدد أبعادَ الثغرات

يميلُ الأشخاص الذين يعملون في تقنية المعلومات إلى إطلاقِ الأحكامِ من منظور التقنية. إن التقنية عادةً ليست بحد ذاتها محلَّ الخلاف، وإنما الخلاف على نحوٍ أدقّ هو في كيف تدار التقنية، أو كيف تؤثِّرُ العواملُ البشرية في استخدام التقنية. تقتضي عملية التقدير، لفهم ثغرةٍ من ثغراتِ وحدةٍ ما، تحديد الأمر الذي يضع هذه الوحدة في خطر.

إن الأشخاص، والتقنية، والعمليات، والبائعين، والقوانين، وشركاء الشركة، وأنظمة البنية التحتية، والمنشآت، والبيئة، والاعتبارات المالية والاجتماعية والتنظيمية قد تُرى جميعها على أنها ثغرات. ولكن النقطةَ الأساسيةَ هنا هي اكتشافُ التهديدات الأكثر احتمالاً التي تتعلق بثغرات الشركة تحديداً. تُستنتجُ الثغراتُ وتُحدَّد بالاعتماد على التجارب السابقة، وطبيعة الشركة، والتنافس، والمكان، ومدى اعتماد الشركة على التقنية، والاعتبارات السياسية والجغرافية، وإلى آخر ذلك.

تقييم أثر ممارسات التخفيف

إن الخطوةَ التالية هي تقييمُ فاعلية استراتيجياتِ التخفيفِ المعتمدة حالياً، وإدخال استراتيجيات تخفيفٍ إضافيةٍ بهدف إدارة المخاطر بشكل فعّال. تتضمن الضوابطُ النافذةُ الاستراتيجياتِ الموجودةَ حكماً في التسلسل الهرمي للضوابط، وقد يكون هناك استراتيجيات تخفيفٍ إضافية ناتجة من نقل المخاطر من جهاتٍ أخرى.

إجمالاً، ستوجد ثغرات وتهديدات متنوعة في دوائر مختلفة من الشركة وتساهم جميعها في إيجادِ المخاطرِ التي يجري تقييمها. قد تتولى عدةُ دوائر في الشركةِ، عندما تسنح الفرصة، عمليةَ تقدير التخفيف المطبَّق حالياً، فعلى سبيل المثال: إن تخفيفَ المخاطر المتعلقة بالتحكُّم بالنفاذِ إلى المعلومات هو في الحقيقة مسؤوليةٌ مشتركةٌ بين تقنية المعلوَمات، ومدراء الشركة، وقسم الموارد البشرية. لا يمكن إبعاد الخطر وتخفيفه ببساطةٍ من خلال طرح برمجياتٍ حاسوبيةٍ جديدةٍ فقط. إذ من الضروري وجود عملية متفق عليها من قبل جميع الأطراف مطورة ومتّبعة من أجل ضمان أن إمكانية النفاذ إلى المعلومات قد تم قطعها، على سبيل المثال: عندما يقوم الموظف بمغادرة الشركة.

حدّد أصناف التخفيف

حدّد العمليات التي تُستخدم حالياً لتخفيف الثغرة أو التهديد. تشير أصناف التخفيف إلى أنواع الضوابط. إن الضوابط الأكثر شيوعاً هي:

- السياسة.
- العملية.
- ممارسة الإدارة.
- الإرشاد.
- إجراءات التشغيل المعيارية أو القياسية (SOPs).

ومن الضوابط أيضاً:

- المعيار التقني.
- العقد.
- المنظمة/ المجلس.
- التدريب.
- القوانين أو القواعد.
- أدوات برمجية.

من المهم أن تتفقَّدَ عملية تقييم أثر الضوابط الحالية أربعَ مناطق جوهرية هي:

➢ **هل توجد ضوابط جاهزة من أجل هذه الثغرات أو هذا التهديدات؟ (أي: هل الضوابط موجودة؟)**

➢ **هل تطبّق هذه الضوابط كما يجب؟** (أي، هل تطبق في كلّ مكان تكون فيه ضرورية؟ هل تطبّق بثبات؟)

➢ **هل الضوابط فعَّالة في إدارة الثغرات أو التهديدات؟ هل كانت الضوابط فعَّالة في التعامل فيما مضى مع مخاطر محتملة مشابهة؟ هل حصل وقوع للمخاطر المحتملة (أي، هل وقعت سابقاً المخاطر) في الماضي؟**

➢ **هل توجد إجراءات وقائية أو ضوابط جاهزة لتخفيف هذه الثغرات أو التهديدات؟ هل كانت هذه فعَّالة في الماضي؟**

قم بصياغة توصيات حول ما يمكن فعله أيضاً لتخفيف الثغرات والتهديدات، وذلك تبعاً لنجاعة الضوابط الموجودة، وفي ضوء الفحص المفصَّل للثغرات والتهديدات؛ فقد تكون هناك ضرورةٌ إلى ضوابط إضافية، وعمليات جديدة و/أو تقنية جديدة. من الواضح أن التوصيات النهائية، التي ستدرج في خطة تخفيف المخاطر، يجب أن تشتمل على تلك الخيارات التي تعطي الربحَ الأمثل و«القيمة المضافة» الأعلى والعائد الأكبر على الاستثمار وعلى الموارد المطلوبة، أي التي تعود بالفائدة الأكبر على الشركة.

بعد وضع التوصيات، المتعلقة بجميع المخاطر، تَحَقَّق من أنها:

ـ مترابطة وتعالج جميع المخاطر.

ـ ستكون مقبولة من هؤلاء الذين سيتعاملون معها يومياً في جميع دوائر الشركة.

ـ لا تتناقض مع الضوابط الموجودة ولا تسبب آثاراً سلبيةً خارج نطاقها.

ـ تأخذ بالاعتبار التكاليف المتوقعة، والخطر المحتمل، والثمرة المرتقبة.

قس الالتزام
وطور أدواته وطرائقه وعملياته

إن قياسَ الالتزام أمرٌ مهمٌ لنجاحِ كامل عملية إدارة المخاطر. حدّد ما إذا كان لطرائق إدارة المخاطر حقاً أثرٌ إيجابيٌ، وكن قادراً على قياس المدى الذي تُستخدمُ فيه فعلياً ضوابطُ التخفيف. من الواضح أن قياسَ الالتزام بالتطبيق أمرٌ شاقٌ، إلا أن ما يساعد في نجاح هذا التطبيق هو سهولة العملية وإدراك فوائدها، وليس لها أثر سلبي. يتم عادة إدخال المدققين للمشاركة في هذه المرحلة من العملية، فالمفتاح الأساسي هنا هو ضمان أن المدققين هم مع العملية، وأن نتائجَهم لن تُستخدمَ ضدَّ الدوائر أو الوحدات التي يجري تدقيقها.

يجب أن لا يُنظرَ إلى مراقبة الالتزام بالتطبيق على أنها وجهُ العقوبةِ في إدارة المخاطر، وهذا هو السبب وراء أهمية إيجادِ وظيفةٍ منفصلةٍ لإدارة المخاطر تكونُ شريكاً مع فريقِ الشركة المدققة. خذ بعين الاعتبار ما يلي عند التخطيط لأدوات قياس الالتزام بالتطبيق:

- نطاق تطبيق قياس الالتزام أي: ما الذي سيتم قياسه، أين ومتى ستتخذ القياسات، ومِنْ قِبَلِ مَنْ؟

- كيفية تأدية الحصول على البيانات، على سبيل المثال: استفتاءاتُ تقييم الذات، أو الأدواتُ المبنية على آلية الـ «ويب» (web-based)، أو المقابلات، أو نتائجُ المراقبة والتدقيق، أو الإحصاءاتُ المستقاةُ من تنفيذ العمليات الروتينية. (لا تستخف بالوقت المطلوب للحصول على البيانات)

- كيفية الحثّ على الإجابة أو الرد، على سبيل المثال: كيفية ضمان أن الاستفتاءات ستحظى بالإجابة، كيفية ضمان عودة البيانات كما هو مطلوب.

- طرائق جمع الردود وتخزينها.

- طرائق قياس الإجابة، أي تحديد كيفية استخدام البيانات لقياس مدى الالتزام.

- تفحُّصُ إجراءات المتابعة الضرورية.

➢ قد يقتضي الأمرُ جمعَ معلوماتٍ أخرى في مهمة التخطيط الأولية هذه، بما في ذلك:

- قائمة جرد لما هو تحت السيطرة حالياً،
- وعملية حل النزاع، وعملية التصعيد.

الخلاصة

إن إدارةَ المخاطر عمليةٌ مهمةٌ للشركة وهي ممارسةٌ إداريةٌ صحيحة. إن استخدامَ ممارساتِ إدارة مخاطر تقنية المعلومات أمرٌ مهمٌ لنجاح الشركة في عصر الأعمال الإلكتروني، لذلك فإن استعمالَ إطار عمل إدارة المخاطر لتقييم أثرها في تقنية المعلومات، يسمح للشركات اتخاذ قرارات منطقية حول المخاطر، ويساعد على تحديد مكان استخدام الموارد لتخفيف هذه المخاطر. الأمر الأخير والأكثر أهمية هو أن استخدام منهجيةٍ مشابهةٍ لتلك المبينة في هذا الفصل يُكَلَّلُ بالنجاح عادةً، فالمفتاح هو استخدام العملية بشكل متماسك وجعلها جزءاً من ثقافةَ المؤسسة.

الوثوق بالأنظمة المعتمدة

«هل نستطيع الوثوق بأحد؟». هو قولٌ شائعٌ في مجتمع أمن المعلومات، ولكن في بعض الأحيان، يحتاج كلٌّ من الأشخاصِ والأنظمةِ أن يثقَ بعضهم ببعض كي يتمكنوا من إرسال المعلومات وتلقيها، وتخزينها، واستخدامها وتحديثها. تتبادل الأنظمةُ في العديد من الحالات معلوماتٍ هامةً خلال بضعِ ثوان (مثل أسواق المال) مستخدمةً مجموعةً من مفاتيحِ التعميةِ أو أماراتَ التصديق التي تثبت هوية كلٍّ منهم. تتأكد عادةً أنظمةُ البَريدِ الالكتروني لدى الشركات من هوية بعضها بعضاً قبل الأخذ بمحتوياتها كي تضمنَ أن الرسائلَ السِّريةَ لن تُنقل إلى حاسوبٍ مخدِّمٍ غير مخوَّلٍ بالاطلاع عليها. ومع استمرار تعاظم إرسال كميات متزايدة من رسائل البريد الالكتروني غير المرغوب فيها (SPAM)، نُوقِشَت العديدُ من الاقتراحات من أجل قيام الرسائل الكترونية بـ «التعريف» عن نفسها قبل موافقة المستخدم على استقبالها، وبذلك سيجري رفضُ الرسائلِ غير المستحبة (غير الموثوقة).

كيف يصبح النظام «موثوقاً»؟ يعتمد ذلك عادةً على طريقتين مستخدمتين:

أ ـ التأكد من أن البرمجياتِ المُدخلةَ على النظام «جيدةٌ ومعروفةٌ» وقد جرى تفحصها والاطمئنان إلى خلوِّها من الفيروسات، والديدان، وأحصنة طروادة ونقاط ضعفٍ أخرى تجعلها غير جديرةٍ بالثقة. بالإضافة إلى ذلك تضاف برمجياتٌ خاصةٌ للتصديقِ أو التعميةِ تسمح باستجابة شرعية لتساؤلات الحماية من قبل الأنظمة التي تحتاج إلى مشاركة المعلومات معها. في معظم الحالات تُجرى اختباراتٌ دوريةٌ لبرمجيات أمن الأنظمة لضمان أنها لا تزال موثوقة.

ب ـ قيامُ جهةٍ مستقلةٍ وموثوقةٍ، مثل «إي ترست» (Etrust) أو «حلول الشبكة» (Network Solution)، بفحص النظام والتأكد بثقةٍ وأمانةٍ من صحة سياسات المنظمة وإجراءاتها المتعلقة بأمن معلومات الزبون. قد تقوم كذلك مجموعةٌ مستقلةٌ، كجزء من ذلك التفحص، بالتأكد من سلامة برمجيات أمن الأنظمة.

تماماً كما هي الحالُ في الوثائقِ الورقيةِ، يجب على المنظمات والشركات أن تقومَ بحمايةِ معلومات الزبون الحاسوبية إلى أقصى درجةٍ معقولةٍ أو عمليةٍ. إن الحصولَ بطريقةٍ غيرِ شرعيةٍ على المعلومات التي تخزن رقمياً أسهلُ بكثير من تلك المخزنة ورقياً، واستخدامها من أجل أهدافٍ متعددةٍ أسهلُ وأسرعُ، ومن الممكن أن تؤخذَ بدون علم المالك، على الأقل لبعض الوقت. تجتمعُ كلُّ هذه العوامل ـ إضافةً إلى قوانين الحكومة حول خصوصية الزبون والاستخدام غير الشرعي لمعلوماته ـ في المستوى الإداري للشركةِ أو المنظمةِ كمتطلباتٍ لحماية المعلومات الخاصة بالزبون من الوصول المحظور إليها وسوء استخدامها.

يتطلبُ تنفيذُ هذه المهمة (إذا كان من الممكن تنفيذها) خبرةَ خبراءِ برامج الحاسوب، ومدراء الشبكة، ومصممي الإنشاءات، ومهندسي أمن المعلومات، والإدارة، وآخرين كُثُر. يحتوي القسم الثالث من هذا الكتابِ على معلوماتٍ حول الأفكار والتقنيات المتنوعة والمتوفرة لحماية البيانات ـ يصف هذا القسم «السَّبَبَ» أو «لماذا».

إن أبسطَ سبب لـ «لماذا» هو توقع سيادة الثقة بين الزبون، والمساهم، والمزود، والمنظمة التي يمدونها بمعلوماتهم. فإذا شكَّت إحدى هذه الجهات بأن معلوماتها الخصوصية قد سُرِّبَت بدون معرفتها أو بدون أذنٍ مسبقٍ منها ـ أو

أنها سرقت ـ من الذي وثق به، فإن لديها طرقاً عديدةً لطلب حُكم قانوني ومالي للتعويض عن الأضرار الحاصلة جرّاء خلل الثقة. إن حماية المعلومات المزودة بناءً على الثقة، من أجل استعمالها في التعاملات بشكلٍ قانوني، تنطوي على مخاطر وفوائد. تكمنُ المخاطرُ في احتمالِ سرقة هذه المعلومات أو إساءةِ استخدامها بطرقٍ غير مخططٍ لها، مسببةً بذلك عقوباتٍ ماليةٍ وقانونيةٍ. أما الفوائدُ فتفوق عادةً المخاطرَ وتتمثلُ بالأرباح المالية من التعاملات المتزايدة، وفرص البيع الأكثر، وفرص البيع البيني، ومن التكلفة المنخفضةِ جداً لخدمة معلومات حساب الزبون وإدارتها.

يفصل (Lewicki and Bunker, 1996) عام 1996م ثلاثةَ أشكالٍ رئيسيةٍ للثقةِ موجودة في سوقِ الأعمال:

1. **الثقة القائمة على الردع**: توجد عندما يقومُ الأشخاصُ أو المنظمات بما قالوا إنهم سيقومون به، نظراً إلى وجود تهديدٍ بالعقوبة إذا فشل الأداء. يوجد هذا النوع من الثقة في المجتمعات المالية، والقانونية والطبية عندما تكون تكلفة خرق هذه الثقة غالية جداً، تشكل التكلفة ردعاً إزاءها.

2. **الثقة القائمة على المعرفة**: توجد عندما يستطيعُ الشخصُ الواثق فَهمَ تصرفات الطرف الآخر والتنبؤ بها من خلال معرفة شيء ما حوله، مثل عندما تُعقَدُ اتفاقيةُ أجهزةٍ مصنعةٍ وفقاً لطلب الزبون أو جواهر مصممة لتناسب حاجات شخص ما.

3. **الثقة القائمة على التشابه**: توجد عندما تَربِطُ الواثقَ بالموثوقِ به رؤى أو معتقداتٌ أو اهتماماتٌ أو أهدافٌ أو استثماراتٌ ماليةٌ متشابهةٌ، أي عند وجود رابطة مشتركة تُخلق بالاستناد إلى معرفة بعضهم بعضاً. ومثال ذلك: مجموعة أعضاءٍ في حزبٍ سياسي، أو في بطاقة ائتمانٍ ترعاها منظمةٌ غير ربحية لخدمة أعضائها.

تنهار الثقة عندما تُسرق المعلومات الخاصة بالزبون، أو تُفقد، أو تُخَّرب، أو يُساءُ استخدامها، وبالطبع من فترة إلى أخرى تفشلُ التقنية أيضاً وتُفقَدُ المعلوماتُ بشكلٍ مؤقت. إلا أنه في الحالات التي يجري فيها، بشكلٍ غير شرعي، نسخُ المعلومات أو فقدانها، أو كشفها للعامة أو سوءُ

استخدامها لأجل منفعةٍ خاصةٍ، تكون الإدارةُ عادةً الخطَّ الأول للاتصال فيما يتعلق بالأسئلة حول كيفية وقوع هذه الحوادث، وما هي خطط منع حدوثها مجدداً.

إذا ما حدث خللٌ في أمن المعلومات، وبغضِّ النظرِ عن حجمه أو أثره، ينبغي أن تُجريَ تحقيقاً شاملاً وتحليلاً دقيقاً للسبب الرئيسي وراء ما حدث، ولماذا حدث، ومن فعل ذلك، وما هو الإجراء الذي يمكن اتخاذه لتجنب حدوثه مجدداً. يجب على الإدارة العليا والمدراء التنفيذيين أن ينهمكوا في هذه الأنشطة ليدركوا درجةَ الخطر التنافسي، والإعلامي، والسياسي، والمالي الذي لَحِقَ بالمنظمة نتيجةَ الخللِ، وكيف يمكن للأثر أن يُكبح أو يُخفَّف.

نظراً إلى أن كمياتٍ متزايدة من الأعمال التجارية تُنجَزُ عبر الإنترنت، يختفي الاتصالُ المباشر بين الشخص والآخر مما يؤدي إلى عدم معرفة من يقوم بشراء المنتجات أو الخدمات. توجد حالياً تقنيةٌ تَكتشِفُ ضرباتِ الشخصِ على لوحة مفاتيح الحاسوب، وتُوصِّفُها مع تصرفاتٍ أخرى يؤديها الشخص عادةً، فتؤدي هذه التقنية بالتالي إلى أن «تبدو» الحواسيبُ بالاستناد إلى هذه المعلومات المرسلة إلى الحواسيبِ الأخرى على أنها أشخاص. قد يكون هذا مقبولاً في الحالات العادية، ولكن في الحالات غير القانونية، مثل سرقة الهوية أو الخداع المتعمَّد للزبون، قد تتحمل الشركات عبئاً مالياً هائلاً، ومن المحتمل أن لا يغطى من قبل التأمين أو المدخرات المالية.

التأكد من المعلومات الرقمية خارج المنظمة

نتيجةً لتزايد إجراء الصفقات والتعاملات الإلكترونية بين جهات لا تعرف بعضها بعضاً عبر الإنترنت وعبر أنظمة الاتصال المباشر، يُطالبُ الأشخاصُ والشركاتُ والمنظماتُ بتقديمِ معلوماتٍ خصوصيةٍ تتعلَّقُ بهم كي يقوموا بتعزيز الثقة مع شركائهم التجاريين. تكون هذه المعلومات في بعض الحالات معقولةً وعامةً كالعناوين، وأرقام الهواتف، والعلاقة مع جهة ثالثة مثل البنوك.

يُمنَعُ الوصولُ إلى الشبكةِ أو النظامِ لأيِّ شخصٍ لا يرغبُ في إعطاء بياناتٍ أمنيةٍ لإثبات هويّته، ويعود ذلك إلى تعاظمِ سرقةِ الهوِّية، والخداع

أو التزوير أو السرقة أثناء الاتصال المباشر. لقد جرى تطويرُ البنيةِ التحتيةِ للمفتاح العام (PKI)(*) كَحَلٍّ لمشاركة المعلومات الخصوصية وتأكيدها بين طرفين لا يريدان تقاسم أسرارهما، ولكنهما بحاجة إلى إجراء تعاملات.

تقومُ منظومةُ الـ (PKI)، التي يشرف عليها طرفٌ ثالثٌ، بتأمين التواصل بين المجتمعات العامة أو الخاصة التي تطالب بكفالات من أجل التحقُّقِ من الهوية وعدمِ إنكار الصفقات. يحتفظُ الطرفُ الثالثُ الموثوقُ بالمفاتيح العامة المستخدمة لفكِّ تعمية الرسائل والصفقات التي يُرسِلُها المستخدمُ مستعملاً مفتاحهُ الخاص. تُوفِّرُ منظومة (PKI) للمستخدمين طريقةً مستقرةً قابلةً للإثبات لتوقيع الوثائق توقيعاً رقمياً، والقيام بمشترياتٍ ضخمةٍ، وإجراء المعالجة الطبية واستخدامات أخرى، وتشابه هذه الحالةُ من حيث الفكرة حالةَ الزبون والتاجر اللذين يضعا ثقتهما بشركة بطاقة الائتمان لإرسال فاتورة حساب الزبون ودفع حساب التاجر.

من المهم أن تكون فوائد تبادل التواقيع الرقمية والملفات الأخرى رقمياً واضحةً للمدراء التنفيذيين وكبار المدراء، فالتوفير في الوثائق الورقية، وفي وقت الانتظار، وفي رسوم البريد قد تبلغ ملايين الدولارات في كلِّ سنة للمنظمات الضخمة، وقد تكون الوفورات هائلة للمجموعات الأصغر. يتطلبُ اعتمادُ منظومة (PKI) موافقةَ المجتمعات القانونية والمالية لتكون ناجحةً تماماً، ولقد بدأ العديدُ من الشركات الضخمة مثل مصرف (سيتي بانك) باستخدام التواقيع الرقمية عندما يكون ذلك مسموحاً قانوناً.

الخلاصة

إن حَوكمةَ أمن المعلومات موضوعٌ عميقٌ وواسعٌ يتطلَّبُ تركيزاً مستداماً على العديد من النشاطات الهامة والإستراتيجية وتلك المتعلِّقةِ بالزبون. فالمخاطر، والمسؤولية، والنزاهة، والثقة، والأخلاق هي فقط بعض من مجالات المسؤوليات التي تواجهها الإدارة العليا بشأن هذا الموضوع، ويتطلب

(*) وهي منظومة تعمية (تشفير) تشرف عليها جهة حيادية مثل الحكومة أو شركة معتمدة تحدد لكل شخص أو شركة مفتاحَ تعميةٍ خاصاً وآخر عاماً، تضمن هذه المفاتيح تحقق كل جهة من هوية الجهة الأخرى قبل تبادل المعلومات.

كلٌّ منها تفكيراً جاداً حول الافتراضات، والاتصالات وردود الأفعال التي تؤثر في أغلب ـ أو جميع ـ دوائر المنظمة.

إن ما يثيرُ الاهتمامَ في جميع هذه المجالاتِ هو الدرجةُ العاليةُ من التكاملِ فيما بينها، ففي أغلبِ الحالات، يتطلبُ المجالُ الواحدُ الدعمَ من جميع المجالات الأخرى. فالقليل منها هي جزرٌ مستقلة، ويعود ذلك إلى تكامل البريد الالكتروني، وأنظمةِ الدعم الحاسوبيةِ التي تمتد عبر كلِّ دوائر المنظمة وعبر سلاسلِ التزويدِ المتكاملة مع الشركة. إن الناحيةَ الإيجابية في كل هذا هي أنه قد يحدث تداعمٌ وتعاضد هائلٌ بين الأنظمة المتكاملة عندما تُطَبَّقُ بنجاحٍ وتدارُ بشكلٍ مسؤول.

كما يمكن أيضاً اعتمادُ ممارساتِ أمنِ معلومات قوية ومتدرجةٍ في كل دوائر المنظمة؛ ففي معظم الحالات يكون الصرفُ على هذه الممارسات تدريجياً وبانتظام أكثرَ ربحاً من الاضطرارِ إلى دفعها لاحقاً لتسوية ادعاءات وإعادة تأسيس مصداقية المؤسسة بعد فقدان الأمن أو حدوث خلل فيه.

إن قرارات الحوكمة وبناءَ هيكلية أمن المعلومات، التي بدورها تؤدي إلى اختيار التقنية، مواضيع سيجري تناولُها في أقسام الكتاب اللاحقة.

إطار عمل الممارسات الأفضل

الممارسة الأفضل (المثلى)	الحساسية	التكرار	المشاركون	نتائج النشاط
هل الوصولُ إلى معلوماتٍ معينةٍ مقصورٌ على الأشخاص الذين يحتاجون إلى معرفتها أو استخدامها؟	عالية	فصلياً (كل ثلاثة أشهر)	الإدارة، أمن المعلومات	ارتباطُ المعلومات المباشر بالأشخاص تبعاً لحاجة الشركة.
هل تم التحقُّقُ من افتراضات الأمن في جميع مستويات المنظمة؟ هل هي مرتبطة بحاجة الشركة؟	**عالية**	**ستة أشهر**	الإدارة، أمن المعلومات، المالية، التسويق	خطَّةُ أمنٍ متكاملةٍ قائمةٍ على حاجة الشركة وتوفُّرِ الاستثمارات.
هل تلتزمُ المنظمةُ بالممارسات الأفضل في المسؤولية، والنزاهة، والثقة، والأخلاق؟	عالية	ستة أشهر	الإدارة، أمن المعلومات، المالية، قسم الموارد البشرية والتدريب	ثقة العامة والموظفين بالمنظمة تؤدي إلى عائداتٍ أعلى، وحصةٍ أكبر من السوق.

يتبـــع

تابـــع

هل تمتلك المنظمة سياساتٍ منطقيةً نافذةً توازنُ بين مراقبة الموظفين وخصوصيتهم؟ هل هي مكتوبة؟	عالية	ستة أشهر	الإدارة، أمن المعلومات	تقليل الالتباس بين ما هو خصوصي وغير خصوصي في العمل
هل هناك خطط جاهزة لنقل الأخبار الجيدة والسيئة إلى الزبائن والمساهمين؟	متوسطة	فصلياً (كل ثلاثة أشهر)	الإدارة، المالية	الثقة في قدرة الإدارة على تحقيق الأهداف وحلِّ المشكلات
هل هناك إجراءات وقائية فعَّالة ونافذة لحماية معلومات الزبون والمساهمين؟	عالية	فصلياً (كل ثلاثة أشهر)	الإدارة، المبيعات، التسويق	شكاوى قليلة من الزبائن حول تسريباتٍ خاطئةٍ للمعلومات الخصوصية.
هل تم تأكيد افتراضات المخاطر من أجل المنظمة؟ هل مازالت دقيقة؟	عالية	ستة أشهر	الإدارة، أمن المعلومات، المالية	مستوياتُ مخاطرَ مخفضة بسبب التحليل الدقيق وتخطيط الوقاية
هل أدواتُ الالتزام بضوابط التعامل مع المخاطر جاهزة وهل يجري استخدامها؟			الإدارة، أمن المعلومات، المالية	عمليات موثوقة، قابلة للتنبؤ بها لتحديد وتقليل المخاطر

القسم الثاني

هيكلة منظومة أمن المعلومات
(قضايا العمارة)

يركزُ هذا القسم على بناء «عمارة» أمن المعلومات بما في ذلك القضايا التي تهمُّ الإدارةَ العليا والمديرين التنفيذيين حولَ كيفيَّةِ ترتيب الأمن، وهيكلةِ البنيةِ التحتية، والتطبيقات، لتحقيق أقصى الفوائد الممكنة. سيناقشُ هذا القسم أيضاً بناءَ حواجز متعددة للحماية، وتحديدُ تهديداتِ الأمن الداخلية، وتخطيطَ التعاملِ مع الكوارثِ في سيناريوهاتِ الحالةِ الأسوأ.

لسوءِ الحظِّ، لا توجدُ خطةٌ معياريةٌ لهيكلة أمن المعلومات تُوسّعُ أو تُختصَرُ كي تُلَبي حاجات أي منظمة. تمتلكُ كلُّ منظمة متطلباتٍ مختلفةً لأمن المعلومات، وقيود مالية خاصة وامكانيات تحمل مخاطر وموارد تقنية خاصَّة بها. قد تَضَعُ شركةُ تجارةٍ إلكترونيةٍ صغيرةٍ خطَّةَ أمنٍ تكلِّفُ مليون دولار لتسدَّ احتياجاتها، بينما قد تنفقُ وكالةٌ حكوميةٌ ضخمةٌ 100 مليون دولار وتبقى تعتقدُ أنَّ هناك نواقصَ أمنٍ هامة لا تزال بحاجةٍ إلى العلاج. إن موازنة هذه العوامل مع توقعات المساهم والزبون هو أمر صعب، كما أن جميع هذه العوامل تتغير كثيراً، غالباً كل يوم وذلك بسبب ظهور التهديدات الجديدة. ولكن على الرغم من ذلك هناك بعض الأمور المشتركة بين أغلب منظمات تقنية المعلومات تسمح بالاستفادة من أطر عمل «الممارسات الأفضل».

تُوضَعُ هياكل أمن المعلومات غالباً تحسباً لتهديدٍ معروفٍ أو وضعٍ متوقعٍ. في معظم الحالات، يكون التفكير الإيجابي الفاعل في طيفٍ واسعٍ من التهديدات والمخاطر المحتملة أربحَ من إعداد وتطبيق الحلولِ المفردةِ التي لا تتعامل بشكل مباشر مع الفرص أو الآثار المرافقة. يأتي الربحُ الذي يفوقُ التكاليف من الاستفادة من تعاضُدِ مجموعةٍ من إجراءاتِ أمنٍ عديدة مثل: جدران النار، ورُقَع مواءمة نظام التشغيل (OS)، وأنظمة الرقابة والتفتيش الآلي، والنفاذ القَائم على الوظيفة، وإدارة موافقات نفاذ متعددة المستويات، والبرمجيات الآلية للحماية من الفيروس... الخ، التي قد

تتعاضد مع بعضها بعضاً لإبعاد انتهاكات أمن المعلومات ومنعها. قد تكونُ طريقةُ الحلول المفردة، أي كلُّ مشكلةٍ على حدة، أرخصَ في البداية، ولكنها أغلى بكثير إذا ما اقتضى الأمرُ معالجةَ مجموعةٍ من المشاكل المختلفة للنقاطِ المفردةِ للتعاملِ مع أنواع شتَّى من الاعتداءات، علماً بأن هذه الحال قد أصبحت هي القاعدة.

تشير اعتداءات الديدان والفيروس على نظام مايكروسوفت (Exchange) خلال السنوات الأربعة الماضية أن امتلاكَ مقدرة نشيطة وفعالة ومُتكيِّفةٍ للاستجابة لمتطلبات الحماية كانت أنجحَ من تطبيقِ طريقةٍ تعالجُ كلَّ مسألةٍ على حدة أو استخدام برمجياتٍ مملوكةٍ أو مطورةٍ من قبل المؤسسة. إذ إن المنظمات التي تعتمد تقنيات أو عمليات أمن «لكل نقطة على حدة» تضطر إلى القيام باستمرار بإعادة التخطيط لعملياتها وطاقمها التقني لمواجهة الاعتداءات والتهديدات غير المعروفة سابقاً التي لم تستطع هذه الطريقة منعها.

إن الخطوةَ الأولى في بناء عملية دفاع قوية هي تحديدُ التهديداتِ المحتملة، ومصادرها، وأثرها الإجمالي في المنظمة ـ وهي فقرات سنأتي على شرحها في نموذج مصفوفة التهديد.

الفصل الخامس

النواحي الهيكلية (قضايا العمارة)

لورنس م. أوليفا

المقدمة

يركزُ هذا الفصلُ على بناء عمارة المعلومات أو هيكلتها، مثل: القضايا التي تقتضي التفكير، وطريقة تناسق إجراءات الأمن، وهندسات البنية التحتية، والتطبيقات لتحقيق الفائدة القصوى، وإنشاء حواجز متعددة للحماية، وتحديد تهديدات الأمن الداخلية، والتخطيط للعودة إلى الوضع السوي بعد كارثة في سيناريوهات الحالة الأسوأ.

لكلّ منظمةٍ خصوصيتها في أمن معلوماتها ومواردها المالية وتحمُّلِها للمخاطر. إن الموازنةَ بين جميعِ هذه العواملِ مع توقعات الزبون والمساهم أمرٌ صعبٌ، كما أن جميعَ هذه العوامل تتغير بشكلٍ متكرر. ولكن على الرغم من ذلك، ثمة بعضُ الأمورُ المشتركة بين أغلب منظمات تقنية المعلومات تسمحُ بالاستفادة من أطر عمل «الممارسات الأفضل».

تُخلق غالباً هيكليةُ أمن المعلومات تحسباً لتهديدٍ معروفٍ أو وضعٍ متوقع. إذ إن التفكيرَ والنشاطَ الفعَّال قبل وقوع الحدث هما غالباً أكثرُ ربحاً مقارنة بتكاليف الحلول المفردة التي لا تتعامل بشكل مباشر مع كلِّ الفرصِ أو الآثار المرافقة.

إنشاء مصفوفة التهديد

يجب على كلِّ منظمةٍ أن تقومَ بإنشاء مصفوفة التهديد كطريقة لتحديد مخاطر أمن المعلومات، والاستعداد لها، وإدارتها. قد تكون هذه المصفوفة بسيطة أو معقدة، ولكن مجرد امتلاكها كأداة واستخدامها سيساعد بشكلٍ هائلٍ عند حدوث مشكلة خطيرة. يبيّن الجدول التالي نموذجاً معيارياً لهذه المصفوفة:

	مصدر التهديد	وقت الاستجابة	مقدار أو قيمة الأثر
خارجي	قرصان	فوري	عال
داخلي	موظف	فوري	عال
غير معروف	إرهابي	فوري	عال
احتيال أو تزوير مالي	زبون	فوري	منخفض إلى عال
حرمان من النفاذ إلى المعلومات	متعدد	فوري	عال
تخريب	متعدد	يعتمد على النوع	منخفض إلى عال

ثمة حاجة إلى مشاركة الإدارة العليا في هذه المناقشات والقرارات لتساعد على الموازنة في القرار بين شيئين متناقضين هما المخاطر والتكلفة، إذ غالباً ما يتخذ هذا القرار من قبل الطاقم التقني الذي قد لا يكون ملماً بالمنظور الشامل للمنظمة. وتُتخذُ غالباً قراراتُ اعتمادِ التكلفةِ من قبل المجموعة التي تموِّل تكلفةَ هذه التحسينات الأمنية، وهي قد تتركُ الدوائرَ أو الوحداتِ الأخرى في المؤسسة مكشوفةً للعودة الأبطأ إلى الوضعِ السويِّ بعد الكارثة، أو في بعض الحالات، تتركها مكشوفةً أكثرَ مما سبق نتيجة إلغاء إجراءات الأمن التي كانوا يعتقدون أنها موجودة.

يجب أن تأخذَ الخطةُ بعين الاعتبارِ الحاجاتِ الخاصةَ لتقنية معلومات المنظمة، ولمساهميها، وزبائنها ومزوديها. فعلى سبيل المثال سوف تعتمد المشفى خطةً مختلفة تماماً عن الجريدة، كما ستكون للمصنع الكيميائي خطةٌ تختلف عن تلك المرسومة لحكومة المدينة.

كلما تمكنت مصفوفة التهديد من تحديد أكبر عددٍ ممكنٍ من الثغرات كانت أفضل، وذلك كي يمكن التعامل مع هذه الثغرات والتقليل من مخاطرها. كما أن الإجراءات المضادة للتهديد، التي تتألف من سياسة ومن عناصر تقنية

وعملية، هي أيضاً جزءٌ مهمٌ من هذه المصفوفة التي تتطلب الدعم والمشاركة من قبل الإدارة التنفيذية. إن تحديد درجة المخاطر من أجل تجنبها أو تخفيفها هو غالباً أمرٌ مكلفٌ وصعبٌ. في كلتا الحالتين، التجنب أو التخفيف، قد تدفع المنظمة فاتورة غالية جداً مع فوائد قليلة للزبائن والمساهمين، اللهم إلا استمرار الشركة بالعمل كالسابق. بينما يعدُّ استمرارُ الشركة بالعمل أمراً إيجابياً، إلا أن عدمَ القدرة على توليد عائدٍ للاستثمار قد يكون عائقاً كبيراً جداً يصعب التغلب عليه، خاصةً إذا ما تجاوزت التكلفة التقديرات.

موائمة الهيكلية مع اتفاقيات مستوى الخدمة

اتفاقياتُ مستوى الخدمة (SLAs) هي عادةً وثائق تعاقدية تحدِّدُ المستوياتِ الدنيا لكلٍ من: توصيل الخدمة الاحترافي، ومدد توفر كلٍّ من الشبكة والحاسوب، ومستوياتِ الأداء، ومستويات القدرات، وبروتوكولات أمن النفاذ، ومجالاتٍ أخرى تهمُّ الزبائن والمزودين ويلتزم الجميع بإتباعها.

في معظم الحالات، يتوقع الزبائن الذين يدفعون تكلفة النفاذ والخدمات أن يعمل النظام 99.999 ٪ من الزمن طوال الـ 24 ساعة يومياً، وعلى مدار الأسبوع، إلا أن مزودي الخدمة يتمنون مستوياتِ أداءٍ أقل صرامة، خاصةً لأن هناك إمكانية تعرضهم لعقوبات مالية عند عدم الوفاء بالأداء المتفق عليه.

على الرغم من وجود طرق عديدة يمكن اتخاذها من أجل دعم (SLAs) بمستويات أداء عالية، إلا أن معظم خبراء الحاسوب والأمن سيوافقون على أن الطريقةَ الأبسطَ والأقل تكلفة هي في تنسيق أو مواءمة الحاسوب والشبكة وهيكلية الأمن ضمن بنية تحتية مشتركة. إن دمجَ هذه العناصر الثلاثة في بنيةٍ تحتيةٍ مشتركةٍ يسمح بزيادة كبيرة في عائد الأجهزة والموظفين، كما يسمح بسيطرة تشغيلية أعظم على عمليات الحوسبة الخاصة بالمنظمة.

تتضمن الحسنات الأخرى لتنسيق أو مواءمة الهيكلية التالي:

- أجهزة وعمليات أمنٍ معيارية.
- نقاط نفاذ للمعلومات من خارج المؤسسة محددة ومراقبة منعاً للاقتحام المحظور.
- تكاليف مخفضة بسبب الحاجة إلى برمجيات وتجهيزات أقل.

• جهود أقل لتدريب الموظفين (بسبب استعمال أجهزة معيارية).

• قدرة على تشخيص المشاكل وحلّها سريعاً، نظراً إلى أن المشاكل تحدث غالباً في الأنظمة ذاتها، وأن تصحيحاً لإحدى المشاكل قد يصحح مشاكل أخرى أُحدثت من قبل ذاك الخلل.

• تحقيقُ أداءٍ أفضل من خلال تَوليفِ العناصرِ المختلفة مع بعضها البعض والذي يؤدي بدورهِ إلى هيكليةٍ عامةٍ متكاملةٍ ليس فيها نقاط احتكاك مثل: برمجيات غير متوافقة من مزودين مختلفين أو شبكات مختلفة مع تشكيلات جدار نارٍ واحد، أو مجموعات بيانات تتطلبُ التقييس وإعادة الصياغة بشكلٍ مستمر.

• اختصارٌ كبير في الوقتِ اللازمِ لدمجِ تقنياتٍ أو تطبيقاتٍ جديدةٍ في منصَّةِ برمجياتٍ معياريةٍ شريطة وجودِ مجموعةٍ مشتركة من البرمجيات البينية، ونقاط نفاذٍ آمنةٍ ومراقبي أداء.

تُعَدُّ اتفاقيات مستوى الخدمة، من منظور الإدارة التنفيذية، وثائق هامة ضرورية الوجودِ، باعتبارها تحدد مستوى أداءٍ مفروض. إلا أن تكلفةَ مدة تشغيل «التسعات الخمس» (99.999) قد تتجاوز الميزانيةَ المرصودةَ من المنظمة. من جهةٍ أخرى، عادةً ما يستهان بتكلفة إدارة اتفاقية مستوى الخدمة (SLA) خلال المفاوضات التعاقدية مع الزبون، رغم أنها تشملُ نفقاتٍ مثل: اجتماعات إدارية متكررة لمناقشة القضايا، وقياس مستمرٍ لمؤشرات النظام وجمعها، وارتفاع الغرامات المالية غير الصحيحة، والمناقشات حول من الذي أو ما الذي سبب حدوث المشكلات. في حالة المنظمات الضخمة وباعتماد مستوى أداء زمني في العقد (SLA) هو «التسعات الخمس»، تقدر التكاليف غالباً بـ 250,000 دولار سنوياً، بما في ذلك تكلفة الوقت الإداري التنفيذي.

تتضمن طرق تخفيض هذه التكلفة ما يلي:

• إنقاص اتفاقية مستوى الخدمة (SLA) إلى مستوى أداء 99.99 ٪ أو 99.9٪ ـ أو 99.9٪ ـ إذ إن الانتقال من مستوى مدة تشغيل 99.99 ٪ إلى مستوى مدة تشغيل تشغيل 99.9 ٪ يؤدي إلى فرق 7.7 ساعات إضافية كل سنة (إلى إجمالي 8.8 ساعة) على أساس 24 ساعة على مدار الأسبوع.

• ترتيب الخدمات حسب أهميتها في أن تحظى بعدم الانقطاع «أيُّ خدماتٍ يجب أن تَشْتَغِلَ 99.999 ٪ زمنياً» مثل جدران نار الشبكة وأنظمة

الأمن، وأي لخدمات يمكن أن تتوقف عن العمل لمدة ثماني إلى عشر ساعات كل سنة للصيانة مثل حواسيب المستودعات والنفاذ إلى الحاسوب المركزي.

● كتابة (SLAs) «مرنة» أو قابلة للتعديل حسب حاجات الشركة أو المنظمة. على سبيل المثال: تحتاج شركات بيع التجزئة عادةً إلى مدة تشغيل 100٪ لمعالجة البيانات أثناء فصل عيد الميلاد، ولكنها قد تقبل مدة تشغيل 99.9 بقية السنة وتدفع بذلك تكلفة عقود (SLA) أقل، وكما يأتي:

النسبة المئوية لمدة جاهزية النظام	ساعات كل سنة
100 (24×7)	8760.0
99.999	8759.9
99.99	8759.1
99.9	8751.2
99.0	8672.4

إنشاء حواجز حماية متعددة الطبقات

تُبنى أنظمةُ أمنِ المعلوماتِ الأكثر فعالية في طبقات حمايةٍ متعددةٍ لإقامة حاجز مستمر ضد أنواع عديدة ومختلفة من الاعتداءات، وهذه البنى بانتشارٍ متزايد. في حالة المنظمات الضخمة التي ترتبط ببوابات متعددة مع الشبكة العامة، وبنقاط نفاذ لاتصال الموظف، وبشبكاتِ دعمِ سلسلةِ التزويد، يتطلبُ القيامُ بتطوير حواجز أمنية متعدد المستويات عادة عدة ملايين من الدولارات للهندسة، والشراء، والتوظيف، والاستثمار التشغيلي.

تتضمنُ الطرقُ التقنية النموذجية لإنشاء نظام أمن متعدد المستويات:

● «**مستوى أساس**»: هو حد أدنى من المعلوماتية يقدمها المستخدم لأجل النفاذ (كأنْ تكون كلمة سرّ مشتركة غير معروفة علانية).

● **طبقة ثانية**: تُحدِد الحاسوب المستعمل للنفاذ إلى الشبكة فتسمح له أو تمنعه من النفاذ (من خلال الملف النصي «cookie» أو أمارة الهوية).

● **طبقة ثالثة**: تُقصِرُ النفاذ على المستخدمين «المعروفين» فقط (أي المستخدمين الذين يستطيعون تقديم معلومات التحقق من الهوية الخاص بهم بدون مشاركة مع أشخاص آخرين).

● **طبقة رابعة**: تمنع إلى حد أبعد وصول الحاسوب أو المستخدم إذا لم يعط إجابات صحيحة عن «سؤال التحدي» الذي يملكه ذاك الحاسوب أو المستخدم فقط. يستطيع الحاسوب تزويد المفتاح المُعمَى الذي أرسل له آخر مرةٍ اتَّصلَ فيها بالشبكة وسيُسأل المستخدم عن كلمة مروره الأخيرة.

● **طبقة خامسة**: يُتطلب من المستخدم توفير مميزاً بيولوجياً قابلاً للتحري مثل بصمة إصبعه، أو بصمة صوته، أو سمة وجهه، أو فحص شبكة عينه أو إمضائه (توقيعه). إن واحداً ـ أو مجموعة مؤلفة من اثنين ـ من هذه العوامل ستشكل مستوى عالياً جداً من الثقة بأن الشخص الذي يريد النفاذ هو حقاً الشخص الصحيح.

من وجهة نظر الإدارة العليا، إن جميع هذه الإجراءات الوقائية تكلف الكثير من المال مع القليل من الفائدة الواضحة أو العائد الملموس إلى المنظمة. إلا أن تكلفةَ عدم حماية أصول المعلومات والأنظمة والشبكات من الاعتداء الخبيث قد تكون هائلةً وفقاً للإحصاءات التي أُجريت من قبل منظماتٍ مختلفةٍ حكوميةٍ وخاصةٍ (في صيف 2003، عانت الشركات الخاصة خسارة تزيد على 3.5 بليون دولار للتعافي من الديدان والفيروسات ([CERT, 2003]). وحتى لو قَدَّرنا أن هذه الإحصاءات عالية وخفضنا خمسها (أي: 20 ٪) فمن الواضح أن التكاليف المالية المتراكمة تبقى ضخمة جداً.

إذاً كيف تُربطُ جميعُ هذه المعلومات في بناءِ حواجزٍ متعددة المستويات؟ يجب أن تَفحَصَ كلُّ منظمةٍ قيمةَ أصولِ معلوماتها وأنظمتها وتُحدِّدَ مقدارَ الاستثمار المعقول من أجل حمايتها. في حالة المنظمات الصغيرة، قد تكون عتبةُ الاستثمار منخفضةً جداً، وتعتمدُ على مزودي خدمة من شركة أخرى لتقديم مرشحات الشبكة لمنع الديدان والفيروسات، مع مستوى أو اثنين للتحقق من هوية المستخدم.

فيما يتعلق بالمنظمة المتوسطة إلى الضخمة التي تمتلك مئات أو آلاف الحواسيب والمستخدمين، فإن حساب عدد وأنواع الحواجز والأنظمة الاحتياطية التي يجب شراؤها، قد يتطلبُ عِدَّةَ أشهرٍ وفريقاً من الخبراءِ المكرسين للأمن يتفحصون بعنايةٍ سياسات المستخدمِ والأجهزةِ الموجودة. حالما يتم تحديد التكاليف، تستطيع الإدارة العليا والمدراءُ التنفيذيون اتخاذ قرار تجاري بشأن النفقات، وجداول الأعمال، والسياسات، وتقنيات التطبيق المعقولة المتعلقة بأصول معلوماتهم، وبموظفيهم، وزبائنهم، ومزوديهم ومساهميهم.

كشف المهددات الداخلية لعمليات أمن تقنية المعلومات

تشير جميع تقارير أمن المعلومات فعلياً إلى أن التهديد الأعظم لأصول المعلومات يأتي من داخل المنظمة. لقد طوَّرَ مهندسو التجهيزات تقنياتٍ تسمحُ للمستخدمين وللأنظمة بنقل كميات ضخمة من المعلومات وحفظها بسرعةٍ وسهولةٍ ورخص. في العديد من الحالات، لا يوجد سجلٌ (يدعى أيضاً «سجل الأحداث») يقومُ بتسجيل حدوث نسخ معلومات أو نقلها إلى نظام المستخدم أو أداة تخزينه مثل ذاكرة تخزين المعلومات (Flash) أو ذاكرة القرص المدمج (CDROM). فقد تُنسخُ جداولُ الرواتب، وملفاتُ المريض أو الزبون أو أصولُ معلومات التقنية الأساسية للمنظمة وتؤخذ خارج البناءِ في بضعِ دقائق. وإذا ما تمكن موظفٌ ما من النفاذ إلى الملفات من خلال وصله مع الشبكة العامة، فإن المعلومات قد تُحَمَّل على حاسوبٍ آخر يبعد مسافة 10,000 ميل من الشركة.

كيف يمكن تحديد التهديدات الداخلية المحتملة وإحباطها بدون تطبيق طرائق نفاذ شديدة القسوة تُقَلِّلُ من إنتاجيةِ المستخدمِ وتنقص من معنويات الموظف؟

أولاً: اضمن وجود سياسةٍ مكتوبةٍ تُفصِّلُ توقعات الإدارة بخصوص استخدام الشركة والاستخدام الشخصي للشبكات والأنظمة والمعلومات. ومن النقاطِ الجوهرية في هذا المقام أن تُحرِّمَ مشاركة كلمة سر المستخدم أو أمارات التحقق من الهوية بين المستخدمين. ينبغي أن تشتمل السياسة على عقوباتٍ رسميةٍ على سوء استخدام أصول معلومات المنظمة وأنظمتها.

ثانياً: اجعل جميع الموظفين يعترفون بأنهم قد تلقوا نسخة من السياسة. من الممكن القيام بذلك من خلال البريد الالكتروني أو أداة جمع البيانات عبر الشبكة.

ثالثاً: فيما يتعلق بقواعد البيانات وأصول المعلومات الأكثر أهمية، اجعل مهندسي أمن المعلومات والمهندسين التقنيين يُفَعِّلونَ إجراءات مراقبة دخولِ النظامِ وتسجيلهِ لكي يقوم نظام الحاسوبِ بحفظِ سجلٍ بمن يدخل إلى قواعد البيانات وأنظمة المعلومات الهامة وما هي المدة التي استمر بها هذا الدخول، يجب أن تتم مقارنة هذه المعلومات بلائحة المستخدمين الذين يسمح لهم بالدخول. ويجب حذف أسماء جميع الأشخاص الآخرين من قوائم الدخول.

رابعاً: يجب أن يراقب مهندسو أمن المعلومات أيَّ تنقلاتٍ مشبوهةٍ لملفات معلومات كبيرة عبر جدران النار للمنظمة، وذلك كجزءٍ من نشاطات

مراقبة الشبكة. عادةً، تُنْقَلُ الملفات الكبيرة على وتيرةٍ واحدةٍ ووفقَ جدولٍ زمني نموذجي معروف. تتضمن الأمثلة على أنواع الملفات هذه سجلات الحساب، والملفات المالية، وسجلات مخزون المزودين والصور الرقمية. يستطيع المهندسون أن يحددوا مالكي معظم هذه الملفات بسرعة ويثبتوا شرعيتهم. يجب أن تُفحَص بدقة جميع أنواع الملفات المنقولة، الأخرى، لمعرفة سبب نقلها، وملكيتها الشرعية وطريقة تخزينها المناسبة. على سبيل المثال: إن الحاسوب المركزي الذي يرسل كشفاً مالياً للحساب بحجم 50 ميغا بايت فصلياً إلى الحاسوب المحمول للمدير المالي (CFO) في آخر يوم من كل فصل هو وضع منطقي، أما حاسوب التسويق الذي يرسل ملفاً بحجم 100 ميغا بايت بأسماء حساب الزبائن والتواريخ الشرائية إلى حاسوب الموظف المنزلي مرة واحدة في السنوات العشر الماضية قد يسترعي الانتباه والتدقيق.

على الرغم من أن أغلب سرقات المعلومات تحدث داخلياً، إلا أن الغالبية العظمى من الموظفين صادقون، ويفعلون أقصى ما لديهم لحماية معلومات الشركة. إذا ما أخذنا بعين الاعتبار الإساءة لسمعة المنظمة التي يسببها اختراقٌ واحدٌ فقط لأمن المعلومات، مثل الذي حصل للمؤسسة الأمريكية للرعاية الصحية (TriWest Healthcare Alliance (Gehrke, 2003، والإساءة للمنتجات مثل وضع رمز المصدر لبعض برمجيات ويندوز 2000 لمايكروسوفت وNT 4.0، على الإنترنت في شباط/ فبراير 2004 (Musgrove, 2004)، فمن المنطقي عندئذ أن تسعى الإدارة العليا والمدراء التنفيذيون إلى الإقلال من فرص حدوث السرقة، فضمان تمتع الأشخاص الشرعيين بالنفاذ الصحيح إلى المعلومات التي يحتاجونها للقيام بعملهم، والتحقق بعد ذلك من الأوضاع غير الاعتيادية ـ التي قد تكون شرعية ـ يساعد على تقليل مخاطر حدوث السرقة غير المعروفة أو سوء الاستخدام.

هل التخطيط للعودة إلى الوضع السَّوي بعد الكارثة أمر مهم؟

أجل، وذلك من أجلِ استمرارِ عملياتِ الشركةِ بعد أن أَثَّرَ حدثٌ رئيسي غير مخطط له في العمليات الجوهرية للشبكة أو الحاسوب. إن القدرةَ على استمرارِ عملياتِ خدمةِ الزبون أو توليد العائد هي غالباً هدفٌ رسميٌ هامٌ لكلٍّ من المنظمة وزبائنها. ستأخذ عودةُ عمليات الشركة إلى المستوى الطبيعي وقتاً أطول، وستكلِّفُ أكثر مما هو متوقع بكثير، إذا لم يكن هناك خطةٌ رسميةٌ جاهزةٌ عند حدوث الأزمة والاضطراب. يرجعُ هذا بشكل كبير إلى عدَّةِ أسبابٍ مثل: الإمداد

والتموين، والتعامل مع المزودين والشركاء، وانتظار وصول الأجهزة والموارد المطلوبة من أجل المساعدة، الاعتماد على خطة عودة إلى الوضع السوي بعد الكارثة قائمة على افتراضات أو معلومات غير كاملة أو غير واقعية.

في معظم الحالات، يُعزِّزُ تخطيطُ التعامل مع الكارثة من القدرات والأجهزة الموجودة، ويُقَلِّلُ بالتالي من نفقةِ الاستثمار، إذ تشارك أجهزةُ الاستعادةِ وأنظمتُها مع أنظمة الإنتاج في إنقاص الوقت اللازم لتطبيقها في حال الطوارئ، بالإضافة إلى تفعيل إجراءات وسياسات الأمن المطلوبة لتعمل بشكلٍ فعال.

إن عمليات الأمن جزءٌ من جهود التخطيط للعودة إلى الوضع السوي بعد الكارثة، فنقلُ سجلات الزبون، وسجلات المزودين، والمعلومات الخاصة بالشركة، يجب أن يجري بدون خطأ لتفادي أي توقف في عمليات الشركة أو ضياع الثقة خلال وقوع حدث غير اعتيادي. كما ينبغي تهيئةُ خططِ التدريب وأنشطتها كي تلائم الحالات المقبولة منطقياً، مع تدريبات تجريبية لجميع المشاركين لاكتشاف نقاط الضعف التي تتطلب التحسين والاستثمار.

يحتاجُ كبارُ المدراءِ إلى المشاركةِ في جلسات التخطيط هذه وفي النشاطات التدريبية والتجريبية ليعطوا الاقتراحات، والنقد، والوضوح لجميع أعضاء فرق الاستعادة والأمن. إن فهم «الأبعاد العامة والكبرى» لكلٍ من الاستثمار والأثر يعطي منظوراً مختلفاً عن التركيز التقني أو التشغيلي فقط، وهذا يؤدي غالباً إلى تحسيناتٍ قد تُغفل إذا لم يحصل هذا الفهم.

إن تخطيطَ العودة إلى الوضع السوي بعد الكارثة هو عمليةٌ غاليةٌ وبالغةُ الأهمية. إنه يفترض ظهورَ سيناريوهات صعبة جداً تتطلبُ المهارات الإدارية الأساسية الأربع نفسها التي ذكرت سابقاً في هذا القسم ـ المسؤولية، والنزاهة، والثقة، والأخلاق ـ لتنفَّذَ بنجاح.

الخلاصة

يجب أن تركزَ عمارةُ أو هيكليةُ أمنِ المعلومات على تهديدات الشركة، والاستمرار التشغيلي وأنشطة استعادة الوضع السوي بعد الكارثة. في العديد من الحالات، يُبدأُ أولاً بتطبيق أو توسيع المحاور العامة المشروحة في نشاطات التخطيط للحوكمة المفصلة في القسم السابق. تركِّزُ هيكليةُ أمن المعلومات على

متطلبات الشركة الواجب دعمها، بالإضافة إلى تحديد وهندسة التكرار في النظم، والمرونة التشغيلية، والبنية التحتية القوية (لاحظ الجدول أدناه).

يُحَوِّلُ مخططو الأمن عالمَ «**ماذا لو**» إلى عالم «**كيف**» مع التقيد بحدود الميزانية، وجدولِ الأعمالِ، والمقدرة التقنية، وذلكَ من خلال حياكتهم لثلاث ضفائر مع بعضها البعض وهي العملية والموارد والتقنية. قد يقولُ البعضُ إن تحدي التخطيط أمرٌ صعبٌ، خاصةً إذا أخذنا بعين الاعتبار الالتباسَ في نوع التهديدات، والمكان الذي قد تصدر منه، والأثر الذي قد تسببه. في بعض الحالات يكون ذلك صحيحاً، وهذا يتطلَّبُ العودةَ إلى الأهداف والافتراضات الأساسية من أجل إعادة إثبات صحتها، أما في القضايا الأخرى فإن التخطيطَ التنظيمي البيني، والتفكير الجاد، هما الطريقة الوحيدة للتغلب على التحديات بنجاح.

الممارسة الأفضل (المثلى)	**الحساسية**	**التكرار**	**المشاركون**	**نتائج النشاط**
تفقَّد مصفوفة التهديد الحالية إزاء الافتراضات الراهنة وتحقق من صحتها	عالية	ستة أشهر	الإدارة، أمن المعلومات	وجود مصفوفة تهديد حية ودقيقة للتخطيط الفاعل أو الإيجابي لردود الأفعال إزاء التهديد
تحقَّق من أن جميع الهندسات (الهيكلة) متناسبة مع اتفاقيات مستوى الأداء (SLAs) القائمة	متوسط	ستة أشهر	الإدارة، أمن المعلومات، عمليات (تقنية المعلومات)، المالية	الاستفادة القصوى من عمليات وموارد تقنية المعلومات
تفقّد حواجز الأمن الحالية لضمان أنها تقدم حماية معقولة إزاء المخاطر المتواجدة حديثاً	عالية	فصلياً (كل ثلاثة أشهر)	الإدارة، أمن المعلومات، عمليات (تقنية المعلومات)	إجراءات وممارسات أمن دفاعية ضد المخاطر الحالية
تفقّد جميع العمليات المتعلقة بحماية موارد تقنية المعلومات من الضرر أو الاعتداء الداخلي	عالية	فصلياً (كل ثلاثة أشهر)	الإدارة، أمن المعلومات، عمليات (تقنية المعلومات)	أضرار أو مخاطر مخففة من مصادر الاعتداء الداخلي
تفقّد وتأكَّد من أن جميع خطط العودة إلى الوضع السوي بعد الكارثة موجودة وقابلة للتطبيق	عالية	ستة أشهر	الإدارة، أمن المعلومات، عمليات (تقنية المعلومات)، المالية	خطة عودة إلى الوضع السوي بعد الكارثة قابلة للتنفيذ تقلل من الأثر في الموظفين، والزبائن، والمساهمين، والإدارة

القسم الثالث

قضايا التقنيـة

نظرة شاملة على القسم

يستعرضُ هذا القسم عدَّةَ **تقنياتٍ** هامةٍ في أمن المعلومات لكل منظمة تمتلك أنظمة معلومات. كُتبَ هذا القسم لإعطاء الإدارةَ العليا والمدراءَ التنفيذيين، الذين يتمتعون بمعرفة بعض نواحي التقنية ولكنهم ليسوا بخبراء، نظرات شاملة حول حماية أنظمة تشغيل الحاسوب، والشبكات اللاسلكية المحلية الداخلية (LANs)، وتقادم البيانات مع الزمن، وتخزين البيانات واستعادتها، والبنية التحتية للمفتاح العام (التعمية/الشفرة)، والمميزات البيولوجية للإنسان (لتَعَرُّفِ هويتهِ)، والبطاقات الذكية.

يهدفُ القسم أيضاً إلى عرضِ التقنيات المقبولة، وواسعة الانتشار في السوق، والمفيدة لمهندسي أمن المعلومات والإدارة العليا والمدراء التنفيذيين عند إعدادهم خططَ المواردِ والميزانيات.

الاستراتيجية الإجمالية

عند الأخذ بالحسبان الأهداف والتقنيات والطرق المتعددة المستخدمة من قبل القراصنة، ومخترقي نظم المعلومات، والمراهقين، والموظفين للنفاذ غير المشروع إلى أصول المعلومات، فإن الإستراتيجيةَ الإدارية لإحباط جهودهم تتطلبُ أيضاً تبنّي مقارباتٍ متعددة. تلعب التقنية، بوصفها حاضرة ومتوفرة دوماً، دوراً جوهرياً في العمل آلياً على: كشف، وإيقاف، وتعيين مكان، وتحديد نوع، وتسجيل، النفاذ الاختراقي غير المسموح به إلى شبكات وأنظمة المعلومات.

تقدم أنظمة التقنية، إذا ما جرى اختيارها، وتنصيبها، وتشكيلها، بشكلٍ ملائمٍ، دعماً طوال 24 ساعة على مدار الأسبوع إلى خبراء أمن المعلومات

والمهندسين؛ إذ يستطيعون عن طريقها تقديم التحليل الضروري والقرارات النهائية المتعلقة بالاقتحامات، أو بإخفاق الأجهزة، أو بخطإ البرمجيات، أو فشل اختبارات الأمن المخططة. بشكل عام، تصنف الحواجز التقنية لتحقيق أمن المعلومات إلى:

- **حماية البنية التحتية**: وهي قاعدةُ المستوى الرئيسي الذي يسمحُ لمستوياتِ الأمنِ الأعلى العمل والتواصل معاً.

- **حماية برمجيات التطبيقات ونظام التشغيل**: حماية برمجيات التطبيقات ونظام التشغيل من التغييرات والتعديلات غير المباحة، وذلك عن طريق إزالة البرمجيات غير الضرورية، وحصر إجراء جميع التغيرات على إدارة النظام في ظل عمليات إدارة البنية.

- **تَفحُّص التجهيزات وتثبيت هويتها**: التحقق من وجود هوية مؤكدة لكل التجهيزات الحاسوبية على شكل رموز مسجلةٍ في مكونات هذه التجهيزات، لا يمكن تغيرها بسهولة أو برخص، وتستخدم في إجراءات التحقق من المستخدم وفي الرقابة.

- **تخطيط تقادم البيانات وإدارتها**: يضمن أن البيانات التي جمعت على مدار سنوات عديدة وخزنت، يمكن قراءتها واستخدامها بنجاح، على الرغم من التغييرات في الأداء، وفي المعايير التقنية.

- **بروتوكولات التخزين الاحتياطي والاستعادة منها**: يخوِّلُ النسخ الدقيق للمعلومات المستخدمة حالياً، من أجل استعمالها من قبل المنظمة إذا ما حدث إخفاق غير قابل للاسترداد لمكونات الحاسوب الصلبة (التجهيزات).

- **الطرق المباحة للنفاذ إلى النظام**: تقدم مستويات عديدة من التحقق من هوية المستخدم، وتهدف إلى ضمان أن الأشخاص والأنظمة المسموح لهم فقط هم من يستطيع النفاذ إلى المعلومات والشبكات.

- **تَفحُّصُ نظام الأمن**: يتأكد من أن أنظمة الأمن تعمل، كما هو مخطط لها، بمقتضى الممارسات، والسياسات والمعايير الصناعية المتفق عليها.

تقدمُ البرمجياتُ والتجهيزاتُ، عندما تطبق على أساس متين من الهيكلية والحوكمة، حمايةً قويةً من التهديدات المتعددة داخل وخارج المنظمة. لا يوجد

بالطبع «حلٌ كاملٌ» لمسألة أمن المعلومات. إن الأسواق المتعلقة بالحاسوب والاتصالات هي أسواقٌ إبداعيةٌ وديناميكيةٌ وتخضعُ لعوامل السوق بشكل كبير، لذلك فهي لا تقبلُ معايير صارمة كالتي تفرضها المقارباتُ الشديدةُ غير المرنةِ.

حماية البنية التحتية

البنيةُ التحتيةُ الحاسوبية، في أغلب المنظمات، هي العصبُ الرئيسي للتواصل ولتقديم الخدمات، وتشتملُ على عناصر مثل: تشغيلِ الشبكة، ونقلِ البيانات الكترونياً، ومكاملةِ نظم البرمجيات المشتراة جاهزة من مزودين مختلفين COTS، وخدماتِ اسم النطاق (DNS)، ودليلِ خدمات الشركة (كلمة سر واحدة عبر جميع الأنظمة) وعملياتِ الدعم المستمرة. يتضمنُ أمنُ البنيةِ التحتيةِ كلاًّ من: الحمايةِ الفيزيائية للتجهيزات الحاسوبية لمركز المعلومات، ومكتباتِ البيانات، وأنظمةِ حفظِ وأرشفةِ المعلومات على الأشرطة والأقراص، ونقاطِ النفاذ الاحتياطية الإضافية للشبكة لتلافي حدوث أيٍّ فشلٍ جرّاء وجود نقطة واحدة فقط. تُوَفَّرُ، إضافةً إلى ذلك، مصادر احتياطية محمية للطاقةِ لضمان استمرار العمليات في حال انقطاع الطاقة الكهربائية العامة بسبب إخفاقات شبكة الطاقة أو مشاكل متعلقة بالطقس.

إن حمايةَ البنية التحتية الفيزيائية نشاطٌ تقليديٌ في (تقنية المعلومات) وقد تم تحقيقه بنجاح؛ إذ توجد تقارير قليلةٌ جداً حول مراكزِ معلوماتٍ تعرَّضت للاعتداء الفيزيائي من قبل إرهابيين أو مقتحمين، وتوجد تقارير أقل عن حدوث سرقاتٍ مادية. لقد كان موظفو الشركة، وفقاً للتقارير المنشورة، وراء جميع السرقات من داخل مراكز المعلومات.

الفصل السادس

أمن المعلومات اللاسلكية

كليفتون بوول

جامعة الدفاع الوطني، الولايات المتحدة الأمريكية

المقدمة

لقد ازدادَ انتشارُ الشبكاتِ المحلية اللاسلكية في العملِ وفي المنزل بشكلٍ مفاجئٍ في غضونِ السنوات العديدة الماضية نظراً إلى ظهورِ البرتوكول (802.11b) كمعيارٍ معتمدٍ من أجل الاتصالات اللاسلكية (Al-Saleh, 2002). تتوفرُ الآنَ مجموعةٌ من منتجاتِ الشبكة اللاسلكية لإقامة شبكة منزلك أو عملك اللاسلكية. لقد تَضاعَفَ، منذ عام 2001م، اعتماد الشبكة اللاسلكية في الاستخدام المنزلي عشرة أضعاف. ويوجد الآنَ أقسامٌ كاملةٌ في محلاتِ بيعِ إلكترونياتِ المستهلك مكرسةٌ لبيع المنتجات الخاصة بمكتب العمل أو المنزل (SOHO).

تَستَخدِمُ الآنَ العديدُ من الشركاتِ الشبكاتِ المحليةَ (LANs) اللاسلكيةَ، كطرقِ النفاذِ المفضلةِ ضمن منشآتهم، وذلك بسبب سهولة إنشائها وتمديدها وتنصيبها وصيانتها ونقلها من مكان إلى آخر (Al-Saleh, 2002). يتطلب تغيير الشبكة باستخدام التقنية اللاسلكية تعديلات قليلة للمحيط المادي. إن استخدامَ الوسائل اللاسلكية لبناء الشبكة يجعلُ إجراءَ توسعةٍ تطويريةٍ كبيرةٍ، مثل توسعة الشبكة الحاسوبية أو النظم الإلكترونية الأخرى، أمراً يسيراً. يتمتعُ مستخدمُ

الحاسوبِ المحمولِ بحريةِ التجوُّلِ هنا وهناك في مؤسسته مع الاحتفاظ بالنفاذ إلى الإنترنت وإلى باقي الشبكة. إن الحلَّ اللاسلكيَّ هو أكثر امتيازاً من تمديد شبكة (Ethernet) السلكية عندما تكون الحواسيب بعيدة عن بعضها بعضاً، ويكون المستخدمون بحاجة إلى النفاذ إلى الشبكة.

هناك نوعان من الشبكات المتوفِّرةِ للمستخدم اللاسلكي: شبكة الحاسوب الداخلية (LAN) اللاسلكية (WLAN) **الخاصة** و تلك **المفتوحة**. تكون أغلب الشبكات الداخلية اللاسلكية (WLAN) مرئية للمستخدمين كافة، ولكنها تتطلب درجات متعددة من التحقق من الهوية لإحراز النفاذ إليها. تقترن عادة الشبكات الداخلية اللاسلكية (WLAN) الخاصة بالمؤسسات التجارية الضخمة، وتصمم بشكل يتطلب من المستخدمين إثبات الهوية للنفاذ إلى الشبكة. يتطلب نوع الشبكات الخاصة استخدام مفتاح مشترك للتحقق من هوية المستخدم، كما يُقَلِّلُ عدد المداخل اللاسلكية لشبكة المؤسسة. إن العديدَ من تطبيقات (SOHO) تتحركُ باتجاه هذا النموذجِ لأَنَّهُ يوفرُ لها مستوىً أعلى من التأمينِ لبياناتها. لا يتطلب نموذج التحقق مِن الهوية ذي النظام المفتوح أي تحقق من الهوية لإحراز النفاذ إلى الشبكة. إذ يبيحُ مالكُ الشبكة لأيِّ مستخدمٍ قريبٍ من الإشارة النفاذَ إلى مصادر الشبكة المتوفرة. في معظم الحالات، يكونُ هذا سهلاً كسهولة الاتصال بالإنترنت واسع النطاق. يوجد العديد من الشبكات التي تمنح، عن غير علم، نفاذ المستخدمين لمصادرها، لأن نقاطَ النفاذ إليها مُشَكَّلة أو مُدارة بشكلٍ غير ملائم.

إن العددَ غير المحدود للمنتجات والمصطلحات يجعلُ فهمَ الأمرِ صعباً، ما هو اللاسلكي، وكيف يمكنه تغيير نظرتك إلى الأمور المتعلقة بالشبكة. يسلط هذا الفصل الضوءَ على المميزات، والتعقيدات والثقافة التي تحيط ببرتوكول (802.11b). وسنورد فيما يلي بعض المصطلحات اللاسلكية التي تشرحُ عملَ شبكات (WLAN)، وبعضاً من الممارسات القادمة والاستثنائية في مجالها، وثغرات هذه الشبكات واستراتيجيات أمنها.

تعاريف

إن المعيارَ (802.11b) هو امتدادٌ للمعيار (802.11) الذي يُطَبَّقُ على الشبكات المحلية (LANs) اللاسلكية، ويحدد سرعة تدفُّقِ المعلومات فيه بـ 11

ميغابايت بالثانية، و حزمة تردد الإرسال بـ 2.4 غيغا هرتز. يسمح المعيار (802.11b) بوظائف شبكة لاسلكية تكافئ تلك التي يسمح بها المعيار (Ethernet) للشبكة السلكية. إن المعيار (802.11) هو مجموعة من المواصفات المطورة من قبل معهد المهندسين الكهربائيين والالكترونيين (IEEE) من أجل تقنية (LAN) اللاسلكية.

- نقطة النفاذ (AP): هي جهاز حاسوبي أو برمجيات حاسوب تعملُ كنقطةِ تَجمُّع لمستخدمي أجهزةٍ لاسلكيةٍ كي يتصلوا بشبكة (LAN) السلكية. إن نقاطَ النفاذِ مهمةٌ من أجل توفير أمنِ معلوماتٍ لاسلكي قوي وتوسيع نطاقِ الخدمةِ للمستخدم اللاسلكي. يدعى هذا أحياناً «**البقعة الساخنة**» اللاسلكية.

- مُعرِّف مجموعة الخدمة (SSID): هو المعرِّفُ الأوحدُ المخصصُ لجميع نقاطِ النفاذِ في الشبكة المحلية اللاسلكية (WLAN). عندما يحاول جهازٌ الكترونيٌ نقالٌ الاتصالَ بنقطةِ النفاذ، فإن اسماً مؤلّفاً من 32 حرفاً يلعبُ دور كلمة سر تمنعُ المستخدمين المحظورين من النفاذ إلى الشبكة.

- الخصوصية المكافئة للشبكات السلكية (WEP): هو برتوكولُ أمنِ معلوماتٍ للشبكات المحلية اللاسلكية المحدد في معيار (802.11b). يستخدم (WEP) في أخفض طبقتين من نموذج الاتصالات المعروف (OSI) ـ طبقة ارتباط البيانات والطبقة الفيزيائي أو المادية، لذلك فهذا البروتوكول ليس أمنٌ من النوع «من نهاية إلى نهاية». تقوم (WEP) بتوفير أمن المعلومات عن طريق تعميةِ البياناتِ عبرَ الموجاتِ اللاسلكية كي تكون محميةً أثناء انتقالها من نقطة إلى أخرى.

- (Wi-Fi) هو اختصارٌ لـ Wireless Fidelity أو «إخلاصٌ لاسلكيٌ» وهو اسمٌ آخر للمعيار (IEEE 802.11b). إنه مصطلحٌ تجاريٌ(*) يستخدمُ بدلاً من (802.11b) وبنفس الطريقة التي يستخدم فيها مصطلح (Ethernet) بدلاً من (IEEE 802.3).

- شبكة الحاسوب المحلية اللاسلكية (WLAN): هي نوعٌ من أنواعِ

(*) أُطلقَ من قبلِ Wireless Ethernet Compatibility Alliance.

شبكاتِ الحاسوب المحلية التي تَستَخْدِمُ موجاتٍ لاسلكية عالية التردد بدلاً من الأسلاك لتتَّصلَ بين العقد. انتشرت شبكات (WLAN) أو Wi-Fi في الاستخدام الخصوصي داخل المنزل أو الشركة أو في الأماكن العامة.

● النفاذ المحمي لـ (Wi-Fi WPA): هي مواصفاتٌ قائمةٌ على معايير تحسين أمن المعلومات تزيدُ بقوةٍ مستوى حماية البيانات والتحكم بالنفاذ لأنظمة LAN اللاسلكية الموجودة حالياً والمستقبلية. وُضِعَت المواصفة (WPA) لتقدِّمَ تعميةً محسنةً للبيانات ولتوفِّرَ التحقق من هوية المستخدم (Wi-Fi 2003).

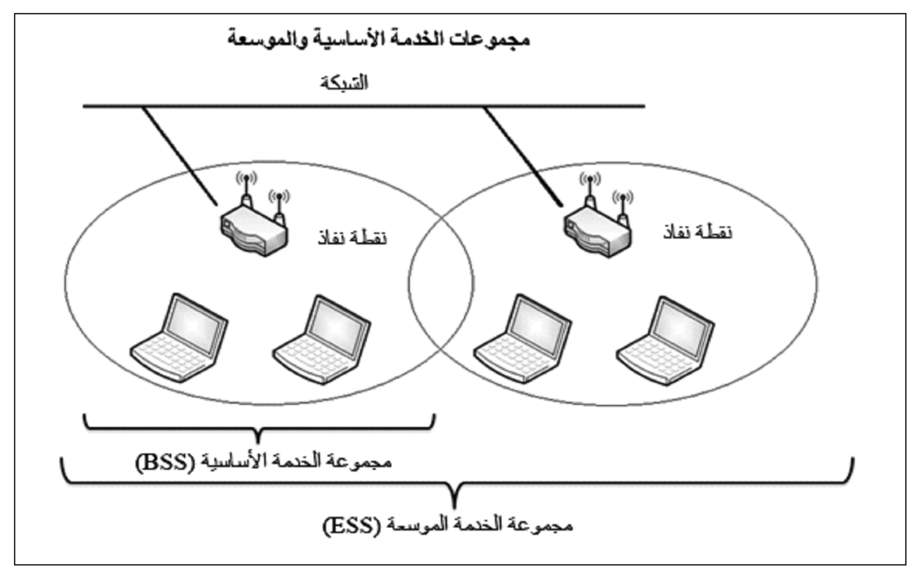
كيف تعمل شبكة (LAN) اللاسلكية

يحدد معيار (802.11b) طريقتين: طريقة البنية التحتية، وطريقة «حسب الحاجة». تتألف الشبكة اللاسلكية في طريقة البنية التحتية من نقطة نفاذٍ واحدةٍ على الأقلِّ متصلةٍ بالبنية التحتية للشبكة السلكية، ومجموعةٍ من محطاتٍ لاسلكية. يدعى هذا التكوينُ أو الهيكلُ مجموعة الخدمة الأساسية Basic (BSS) Service Set (الشكل 1)، وتختص كل مجموعة خدمة أساسية (BSS) بمعرِّفِ مجموعة الخدمة (SSID). إن مجموعةَ الخدمة الموسعة (ESS) هي مجموعةٌ من اثنتين أو أكثر من مجموعات الخدمة الأساسية (BSSs) مُشَكِّلَةً بذلك شبكةً ثانويةً واحدةً تشترك في (SSID).

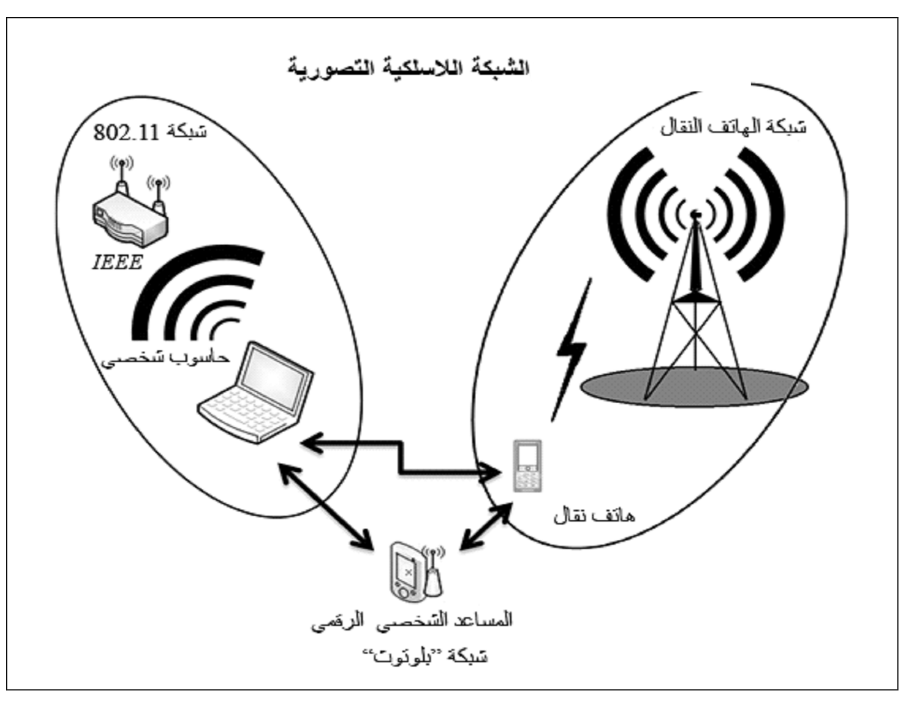
ونظراً إلى أن أغلبَ الشبكات اللاسلكية للشركات (WLANs) تتطلبُ النفاذَ إلى شبكة (LAN) السلكية للوصول إلى الخدمات (مخدمي الملف، والطابعات، وروابط الإنترنت)، فإنها ستعمل ضمن نموذج البنيةِ التحتية. تغطي نقاط النفاذ عادةً مسافة 300 إلى 500 قدم، ويختلف عددها لتشكيل WLAN وفق طريقة البنية التحتية تبعاً للأمور التالية: مساحة المنطقة المطلوب تغطيتها، وتشكيل الشبكة، والحدود الفيزيائية لمناطق التغطية، وعدد المستخدمين لكلّ جزء منها (الشكل 2).

إن الطريقةَ الثانية أي طريقة «حسب الحاجة»، تدعى أيضاً طريقةَ المثيلِ للمثيل، أو مجموعةَ الخدمةِ الرئيسيةِ المستقلة (IBSS)، هي ببساطة مجموعةٌ من محطاتٍ لاسلكيةٍ وفق المعيار (802.11) تتصل بشكل مباشر مع بعضها

بعضاً بدون استخدام نقطة نفاذ أو أي اتصال بالشبكة السلكية.



الشكل (1).



الشكل (2).

إن هذه الطريقة مفيدةٌ في حالات الحاجة لإنشاء شبكة لاسلكية بسرعةٍ وسهولةٍ في مكانٍ لا توجدُ فيه بنيةٌ تحتيةٌ لاسلكيةٌ، أو تكون فيه غيرُ ضروريةٍ لتقديم الخدمات مثل: صفوف التعليم، وغرف الاجتماعات، والمطار، أو حيث يكونَ الوصول إلى الشبكة السلكية متعذراً (مثل المستشارين في موقع الزبائن). تعمل طريقة (IBSS) جيداً في غرفة الصف من أجل مشاركة الملفات بين أعضاء فريق المشروع أو إحالة العمل المنجز إلى الملف المركزي على حاسوب المعلم.

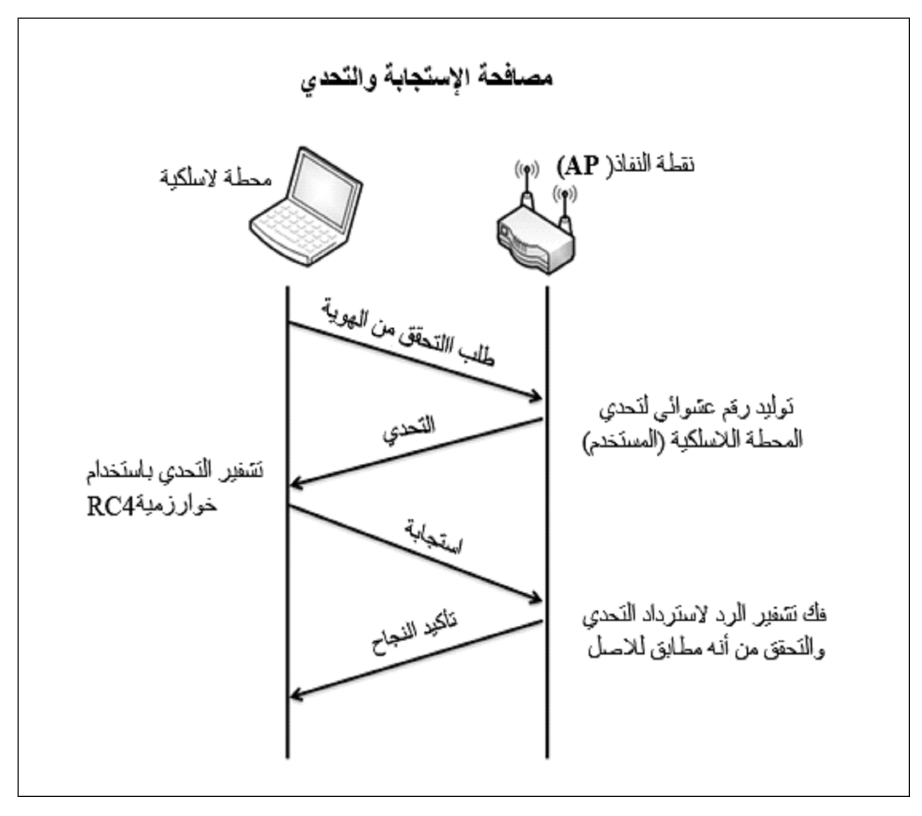
للاستفادة من المعيار (802.11b) في أيٍّ من الطريقتين المذكورتين يتوجب عليك أن تقتنيَ في جهازك بطاقةَ الربط مع شبكة اللاسلكية Network Interface Card (NIC)، تُنَصَّبُ بطاقةُ (NIC) في شقِّ البطاقةِ الصغيرة في الحاسوب (PCMCIA)، وتُبرمجُ للاستخدام مع شبكة (WLAN)، وتأتي الحواسيبُ الحديثةُ مجهزةً بهذه البطاقة (Wi-Fi) كجزءٍ من التكوين النظامي ولا تتطلَّبُ بطاقة (NIC).

يَنْفُذُ المستخدمون إلى شبكة (WLAN) عن طريق نظام تَعَرُّفِ الهوية. يمتلك بروتوكول (802.11b) وسيلتين لِتعرُّفِ هوية المستخدمين: تَعرُّف النظام **المفتوح** وتَعرُّف **المفتاح المشترك**.

لا يُطلبُ منك تَعَرُّفَ هويتك كي تصبح عضواً في شبكة (WLAN) (الشكل 3)، التي تعملُ كنظام **مفتوح**. إذ يرسل المستخدم ببساطة عنوان (MAC) فقط لإحراز النفاذ. وهنا يُفتَرَضُ أن يثق المستخدم بأنه يتصل مع نقطةِ نفاذٍ واقعيةٍ بدون وجود وسيلةٍ فعليةٍ للتحقق من ذلك. لا يُمنح المستخدم النفاذَ للشبكة غالباً لأن مُعَرِّفَ مجموعةِ الخدمة (SSID) يكون غير معروف، أو غير مُمرَّرٍ من نقطة النفاذ كما يجب، إذ من المهم معرفة المحدد الأوحد لأجل ضمان النفاذ. تُنفَّذُ هذه المصافحة أوتوماتيكياً في أغلب التطبيقات بدون علمِ المستخدم.

في نظم التحقق من الهوية وفق طريقة **المفتاح المشترك** تُستخدمُ تقنية «تحدي ـ استجابة» لمنحِ النفاذ إلى شبكة (WLAN). يبيّن كل من كاريجينيس وأوينس (Karygiannis and Owens, 2002) أن المستخدمَ يستعملُ مفتاحاً مشفراً مشتركاً مع نقطة النفاذ فيشفرُ التحديَ المرسل من الشبكة ويعيدُ النتيجةَ إلى نقطة النفاذ. تقومُ نقطةُ النفاذِ بفكِّ تشفير النتيجة المحسوبة من قبل المستخدم وتسمحُ بالنفاذِ فقط إذا كانت القيمة التي فُكَّ تشفيرها تتطابقُ مع التحدي العشوائي المرسلِ في البداية، إن طريقةَ التحقق من الهوِّية هذه هي تقنيةٌ بدائيةٌ في التشفير،

كما إنها لا تزود تحقيقاً متبادلاً، ذلك يعني أن المستخدمَ لا يتحقَّقُ من هوية نقطة النفاذ (AP)، ولذلك فلا يوجد ضمان بأن هذا المستخدم يتصل بنقطة نفاذ وبشبكة لاسلكية شرعيين: وينظر لهذا كسيئَّةٍ في النظم اللاسلكية الحالية.



الشكل (3).

إن أمن المعلومات هي السيئة رقم واحد في استعمال شبكات (WLAN). تَمْنَحُ شبكات (WLANs) فرصاً هائلةً للمخترقين لاقتحام معلومات المؤسسة، يشار إليها غالباً بـ «الغرب الضاري المتوحش»(*) للشبكة. إن تركيب شبكة (WLAN) يشابه وضعَكَ لقطعةٍ من كابل الشبكة خارج نافذتك مع لافتةٍ تقول: «اتصال حر بالإنترنت». قد يرغب أشخاص باختبار الخط ليروا ما إذا كان فعّالاً. فور اكتشافهم لفعالية الخط، سيحاولون توسيع نفاذهم وامتيازهم بقدر ما يسمح

(*) كناية عن ضراوة هذه الظاهرة.

به أمن شبكة (LAN) السلكية. لقد غَطَّت السيئات على الحسنات المكتسبة جراء تركيب شبكة (WLAN).

إن الحسنات هي:

- **قابلية التحرك**: إن المستخدمين ليسوا مقيدين بمكانٍ واحدٍ، فهم قادرون على الوصول إلى الملفات، ومصادر الشبكة، والإنترنت بدون الحاجة إلى الاتصال بالشبكة فيزيائياً بواسطة الأسلاك.

- **تزايد الإنتاجية**: يعمل مستخدمو الأجهزة أو الحواسيب النقالة بشكل أكبر لصالح الشركة عندما لا يكونون داخل البناء، فستجدهم يعملون في القطارات، والطائرات، والباصات والسيارات، فبعض المستخدمين يكون أكثر إنتاجاً فور ذهابهم إلى خارج المساحات الضيقة للمكتب إلى مناطق عامة أكثر راحة.

- **التركيب أو التنصيب السريع**: يَنْخَفِضُ الجهدُ اللازم للتنصيب لأن اتصالات الشبكة تركَّب على الفور تقريباً، فلا حاجة إلى إزالة أية جدران، ولن يُرْسَلَ أحدٌ إلى الأرضيات أو السقوف لسحب الأسلاك، ولا توجد أية تعديلات لازمة لعلبة الأسلاك.

- **المرونة**: يستطيع المستخدمون نصب شبكة (WLAN) صغيرة بشكل سريعٍ من أجل حاجاتٍ مؤقتةٍ مثل: غرفة الصف، أو مؤتمر، أو أحداث مؤقتة أخرى.

- **قابلية التوسعة أو القدرة على تغيير حجم الشبكة**: من الممكن تركيب شبكة (WLAN) بسهولة لتلبي حاجات وتطبيقات معيّنة، كما يمكن تغيير حجمها من شبكات المثيل للمثيل الصغيرة إلى شبكات المؤسسة الضخمة جداً التي تغطي مساحة واسعة.

الممارسات اللاسلكية

يقضي القراصنةُ وقتاً لا بأس به في استغلال الشبكات اللاسلكية. بدأ القراصنةُ أولَ ما بدأوا بما يسمّى «التحرّي بالهاتف» ـ الاتصال بأرقام هواتف إلى أن يجدوا «موذماً» مفتوحاً للنفاذ إلى الشبكات. لقد خلق ازدهارُ الإنترنت في التسعينيات طرقاً مباشرةً وسهلةً جداً للاعتداء مثل: متفحص بروتوكول الإنترنت، ومكتشف الرسائل أو شمّام كتل المعلومات. إن شبكات (LANs) أكثر أمناً من شبكات (WLANs) لأن (LANs) محمية إلى حد ما بطبيعة بنيتها

الفيزيائية، نظراً إلى أن بعض أو جميع أجزاء الشبكة مُتوضّعة داخل البناء الذي يمكن حمايته من النفاذ المحظور، أما شبكات (WLANs) الموجودة عبر الموجات اللاسلكية فهي لا تمتلك البنية الفيزيائية ذاتها، ولذلك فإنها أكثرُ عرضةً للتلاعب. يسمح بروتوكول (802.11b) النفاذَ بسهولةٍ للمستخدمين جميعاً، الموثوقين وغير الموثوقين. لقد تسبب هذا الانفتاح بظهور الجيل الثاني لاقتحام الشبكة المعروفة باسم «التحرّي بالسيارة».

تُنفَّذُ «التحرّي بالسيارة» باستعمال حاسوبٍ محمولٍ مزودٍ «ببطاقة الربط مع الشبكة» (NIC) وببرمجيات قرصنة، وبالتجوال بالسيارة لالتقاط إشارات شبكة (WLAN) غير محمية. في هذه المرحلة من اللعبة يشن قراصنة التحرّي بالسيارة هنا وهناك عملياتٍ للبحث عن ـ أو خطف الشبكات «LAN Jacking» كما تسمى أحياناً ـ شبكات لاسلكية من أجل النفاذ المجاني إلى الإنترنت السريعة مع إخفاء الهوية. يقود، بشكل روتيني، سائقو التحرّي على شبكات (LAN) اللاسلكية سياراتهم المجهزة بحواسيب محمولة مشحونة ببطاقة (LAN) اللاسلكية، وبهوائي خارجي ذي ربحٍ عالٍ، وبجهاز استقبال النظام العالمي لتحديد الموقع (GPS). تُلَقِّمُ كلٌ من بطاقة شبكة (LAN) اللاسلكية، وجهاز الاستقبال المحدد للموقع، الإشاراتِ إلى داخل البرمجياتِ المجانيةِ، مثل برنامج «عاثر النت» (Netstumbler) لاكتشاف نقاط النفاذ ومُعرِّف مجموعة خدمتها ومواقعها المستنتجة من الـ (GPS). إن شكلاً آخر للتحرّي بالسيارة هو التحرّي بالطائرة، حيث تكون أداة النقل طائرة بدلاً من سيارة. لقد شاع مؤخراً تجُولُ الطلاب في الأماكن الجامعية مع حواسيب محمولة مجهزة ببرمجيات فاحصة لتحديد مكان نقاط النفاذ في الأبنية. لقد انتشر نشاط تحديد مكان نقاط النفاذ في السنوات القليلة الماضية انتشاراً كبيراً.

يَستخدمُ القراصنةُ، لتحديد أمكنة نقاط النفاذ (AP)، تقنيةً تدعى تحرّي الحوار (www.warchalking.org) (الشكل 4). إذ إنهم يستخدمون ببساطة الحوار لوضع رمزٍ خاصٍ على رصيف المشاة، أو على سطحٍ آخر، يشير إلى وجود شبكةٍ لاسلكيةٍ قريبةٍ، خاصة تلك التي تمنح وصولاً للإنترنت. إن التحرّي بالسيارة وتحرّي الحوار نشاطان يمكن النظر إليهما على أنهما «ثقافة ثورية جديدة»، باعتبار أن الجمهور المستهدف ليس مالك الشبكة المستهدفة. خلال السنتين الماضيتين تكاتفَ العديدُ من الأشخاص لدعم «يومٍ عالمي للتحرّي

بالسيارة»، حيث يزود جميعُ المشاركين البياناتِ من تجربتهم في التحرّي بالسيارة إلى قاعدةِ بياناتٍ مركزية. تُبَشِّرُ هذه الفكرة بنجاحٍ تجاريٍ عظيمٍ حيث شهدَ العديدُ من بائعي التجزئة، بما فيهم مثلاً مقهى (Kinko's & Starbucks) جاذبية وفائدة هذه الأجهزة اللاسلكية وتبنوا هذه النزعة الأحدث، ألا وهي: البقع الساخنة.

النَّزَعات

إن البقعَ الساخنةَ هي عقدٌ لشبكةٍ عامةٍ وفق المعيار لـ (802.11b) متاحة للمستخدمين اللاسلكيين، وتوضع غالباً في أماكن مأهولة بشكل كبير مثل المطارات، ومحطات القطار، والمتاجر، وأحواض إرساء السفن، ومراكز الاجتماعات والفنادق. تمتلك البقعُ الساخنة عادةً مدى قصيراً للنفاذ وهي متاحة على موقع جغرافي محدد. توجد آلافٌ من هذه المواقع التي تقدم نفاذاً لاسلكياً منخفض التكلفة أو مجانياً إلى مصادر الإنترنت والشبكة.

دعونا نقوم بتحري الحوار...!	
الرمز	المفتاح
SSID)(Bandwidth	عقدة مفتوحة
SSID ○	عقدة مغلقة
SSID access contact (W) Bandwidth	عقدة WEP
blackbeltjons.com/warchalking	

الشكل (4): رموز تحرّي الحوار <http://www.warchalking.org/story/2002/8/20/17730/3808>.

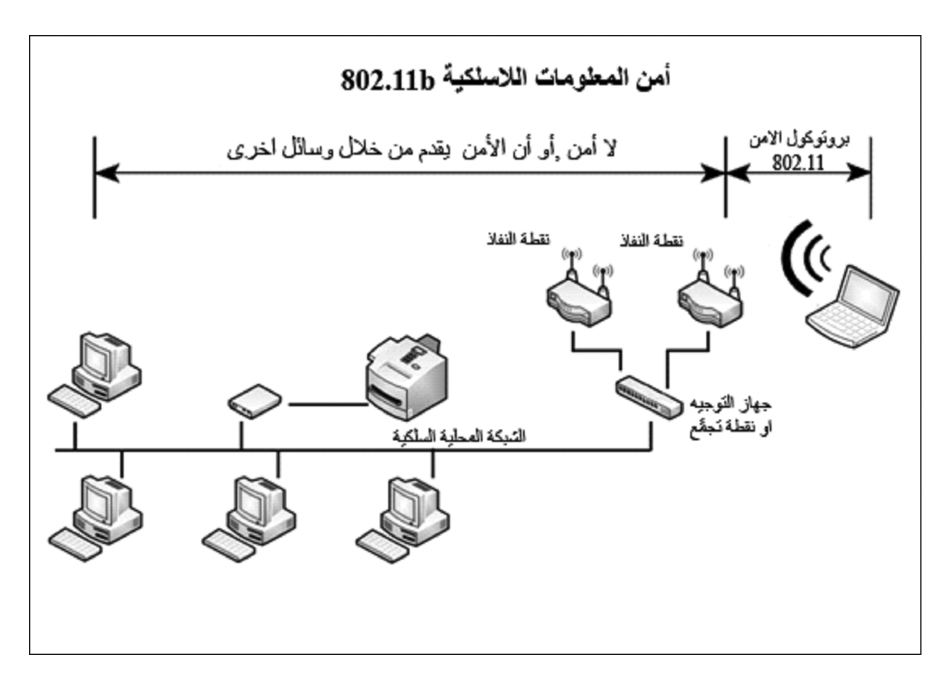
ستقوم البقع الساخنة بتغيير ثقافتنا من خلال تزويد نفاذٍ للإنترنت ذي سرعةٍ عالية في أي مكان وفي كل الأوقات. لقد اتخذ العديد من تجَّار التجزئةِ قراراً تجارياً بتنصيب بقعٍ ساخنةٍ بغية زيادة مبيعات منتجاتهم. تستخدمُ كلٌّ من الفنادق الوطنية والعالمية، والمخابز، والمقاهي النفاذ المجاني لجذب المستهلكين أملاً في بيع قدرٍ أكبر من القهوة والمعجنات أثناء استعمال المستخدمين لنقاط نفاذ عالية السرعة، حيث يتمتع المستخدمون بالنفاذ السريع إلى الخارج وبالاتصال بشبكة خصوصية افتراضية (للشركة التي يعملون بها مثلاً)، كما يستطيعون أن يصلوا بسهولة إلى مكتبهم لاسترجاع المحتوى من الشبكة المشتركة. لقد خلقَ استخدامُ البقع الساخنة ثقافةً جديدةً لدى المستخدمين الذين يعتقدون بأن النفاذ اللاسلكي يجب أن يكون عاماً ومجانياً.

لقد خططت منظمات في الولايات المتحدة، مثل المنظمة اللاسلكية المشتركة وشركائها في مشروع الشبكة اللاسلكية المشتركة، لأن تقوم بتقديم نفاذ لاسلكي مجاني إلى الجميع (http://www.communitywireless.org). تقتني، وفق هذه الخطط، العديدُ من المجموعات والأفراد المحتوى والحزمة العريضة ويتيحونها لمجتمعهم مستخدمين تقنية الشبكة المحلية اللاسلكية وفق المعيار (802.11) (الشكل 5) ذي الوصول المجاني وبرمجياتٍ جاهزةٍ ليس عليها حقوق ملكية فكرية COTS. يوجدُ الآنَ عددٌ من الشركاء في مشاريع عبر الكرة الأرضية يعتقدون أن الشبكة اللاسلكية هي للعامة، ويأملون باستمالة دعم المجتمع التجاري لهذه الفكرة.

الثغرات

تنطبق جميع الثغرات الموجودة في الشبكة المحلية السلكية التقليدية (wired LAN) على التقنيات اللاسلكية (Karygiannis and Owens, 2002). يجب أن يقوم المدراء بمعالجة ثغرات الشبكة المحلية اللاسلكية (WLAN) بقدر أكبر من الحذر، مثل: نقاط الضعف في البنية أو التنفيذ أو التصميم أو إدارة الشبكة أو النظام. تُواجِهُ الشبكات اللاسلكية تحديات خاصة بها عند محاولة تخفيف التهديدات، وهي أيّ شيء قد يعطّل العمل القويم للشبكة أو النظام، فالأجهزة اللاسلكية تسببُ مشكلاتٍ أكثر جرَّاء طبيعتها المتحركة. إن هذه الأجهزة تنتقل من شبكة إلى أخرى، مُتَّصلةً بالإنترنت وعائدةً إلى شبكة (WLAN) المشتركة

مع احتمالية نقل جميع أنواع البرمجيات الخبيثة. إلى حد ما، يجب أن يُعْتَبَر مستخدمو الحواسيب النقال بمثابة «ناقلين للبرامج الخبيثة» وأن يتم عزلهم بشكل إلزامي على الفور في منطقة «معزولة» إلى أن يتلقوا فحصاً ملائماً لإزالة جميع البرمجيات الخبيثة المعروفة (malware).



الشكل (5).

قد ينقل المستخدمون برامجَ خبيثة (malware) لا شعورياً، ويصيبون بالعدوى الشبكة المحلية المشتركة (LAN) إذا لم تتخذ الإجراءات الوقائية المناسبة.

تُحدد النشرة الخاصة لـ (800-48 NIST) بعضاً من أكثر الثغرات والتهديدات شيوعاً في الأجهزة اللاسلكية، لقد صُنِّفَت بشكلٍ يوضح مبدأ أمن المعلومات الذي قد أُخلَّ به عندما لا يجري تخفيف هذه الثغرات والتهديدات كما يجب.

تَحدُثُ انتهاكات السِّريةِ إذا:

- جرى التنصُّتُ على المعلومات الحساسة غير المشفرة (أو المشفرة بتقنيات تشفير ضعيفة) والمنقولة بين جهازين لاسلكيين، وتم كشفها.

• انتَهَكَت الكياناتُ الخبيثةُ خصوصيةَ المستخدمين الشرعيين واكتَسَبَت القدرةَ على تَعَقُّبِ حركاتهم الفعلية.

• كُشِفَت المعلومات الحساسة نتيجة سرقة الأجهزة الصغيرة المحمولة، التي عادةً ما تسرق بسهولة.

تتعرض سلامة المعلومات للشبهةِ إذا:

ـ حَصَلَت الكياناتُ الخبيثةُ على النفاذ المحظور، إلى شبكة حاسوب مؤسسة، من خلال وصلة لاسلكية متجنبين تقنية الحماية بجدار النار.

ـ سرقَت الكياناتُ الخبيثةُ هويةَ مستخدمين شرعيين ودخلت على الشبكات الداخلية أو الخارجية للشركة.

ـ تَخرَّبت البياناتُ الحساسةُ أثناء المزامنة الخاطئة.

ـ سُرِقَت البيانات خِفيَةً من الأجهزة المركبة بشكل خاطئ.

ـ أَفسَدَت الفيروسات، أو البرمجيات الخبيثة الأخرى، البيانات الموجودة على حاسوب لاسلكي، ثم أُدخلت إلى شبكة سلكية عند نفاذ هذا الحاسوب لها.

تنخفض الجاهزية إذا :

ـ وُجِّهَت اعتداءاتُ «الحرمان من الخدمة» (DOC) إلى الوصلات أو الأجهزة اللاسلكية.

ـ اتَّصَلَت الكياناتُ الخبيثة، من خلال شبكة لاسلكية، بمنظمات أخرى في سبيل شن الهجمات مع تعمية نشاطها.

ـ كان المتطفلون، سواء من الداخل أو الخارج، قادرين على إحراز الدخول إلى ضوابط إدارة الشبكة، وبذلك يضعفون أو يعطلون العمليات (النشر الخاص بـNIST 48-800).

تزداد حالياً حاجة الشركات إلى حلول أقوى لأمن المعلومات نظراً إلى أن شبكات (WLAN) قد أصبحت واسعة الانتشار. إن ما أُثبِتَ مؤخراً حول وجود ثغرةٍ في تعمية «الخصوصية المكافئة للشبكات السلكية» (WEP)، قد جعل الأمر واضحاً، أي أن حماية (WEP) وحدها غير كافية، فمواصفات الأمن في (WEP) لا تمنح مستوى عالياً من الحماية. لقد نَشَرَ الثلاثي فلوهرر ومالتين وشامر

(Fluhrer, Mantin and Shamir, 2001) طريقةً لكسر شفرة تقنية خوارزمية RC4 المستخدمة في (WEP) باستعمال «النص المعمى». لقد صرح هؤلاء المؤلفون «لاحظوا أننا لم نحاول مهاجمة اتصال فعلي لـ (WEP) ولذا لا ندعي أن (WEP) هو عرضة لهذا الاعتداء فعلاً». ولكن فيما بعد، نفَّذَ ستبلفيد، لونيديس وروبن (Ioannidis and Rubin, 2001) كسر هذه التقنية بنجاح مثبتين وجود هذه الثغرة في (WEP).

ليس هناك داع للغضب بشأن أخطاء التصميم المكتشفة في (WEP)، فـ (WEP) تفعل ما صممت لتقوم به كخدمة أمن معلومات. إنها تقدم، كما يشير الاسم، مستوى حماية وخصوصية مكافئ لمستوى حماية وخصوصية مستخدمي (LAN) السلكية. لم تكن الضمانات موجودة، وفي حين إعلان هذا المعيار لم يكن هناك أي شخص يطالب بمواصفات أمن أكيدة. من أجل شبكات (WLAN) قام معهد IEEE بتعين WEP لتأدية الوظائف الثلاث الآتية:

ـ **التحقق من الهوية**: لقد كان الهدفُ الرئيسي لـ(WEP) تقديمَ خدمة حماية للتثبُّت من هوية المحطات المتصلة. يزود هذا تحكماً بالنفاذ إلى الشبكة بوساطة رفض وصول محطات حاسوبية لا تستطيع القيام ببيان هويتها كما يجب. توجِّهُ هذه الخدمة السؤال «هل يُسمح فقط للأشخاص المباحين بالدخول إلى شبكتي؟».

ـ **السِّرية**: لقد كانت السِّرية أو الخصوصية الهدف الثاني لـ (WEP). فلقد طُوِّرَت لتقديم ذات «الخصوصية المحققة بوساطة الشبكة السلكية». إن الغاية كانت منعَ كشف المعلومات عن طريق التنصت العرضي (الاعتداء السلبي). توجه هذه الخدمة السؤال «هل يسمح للأشخاص المباحين فقط برؤية بياناتي؟».

ـ **سلامة وصول البيانات**: إن الهدف الآخر لـ (WEP) كان خدمةَ أمن المعلومات المطورة لضمان عدم تغيير الرسائل خلال الانتقال بين الحواسيب اللاسلكية ونقطة النفاذ في الاعتداء الفعال. توجه هذه الخدمة السؤال «هل البيانات الداخلة إلى الشبكة أو الخارجة منها جديرة بالثقة ـ هل تم التلاعب بها؟» (Karygiannis and Owens, 2002).

تعود أغلبُ المآخذ على أمن شبكات (WLAN) إلى الأخطاء الموجودة في **تصميم** التقنية أو **المواصفة**. من الصعب إصلاح نقاط الضعف الموجودة في

التصميم حالما يتم شراء المنتج. إن جميع التقنيات عُرضَة لوجود خطأ في التصميم، وللتغلب على ضعف التصميم ينبغي على مدراء (WLAN) أن يحتاطوا على نحو إضافي لبناء وتنفيذ وإدارة الشبكة كما يجب. من المستحيل تحديد جميع الثغرات المحتملة بشكل نهائي عندما يتم شراء المنتج وقبل إضافته إلى الشبكة. ولكن يوجد وقتٌ كافٍ فور شرائه لإجراء تعديلات طفيفة على البنية أو التنفيذ بإدخال ممارسات إدارية فعّالة. تناقش الفقرة التالية الأنواعَ المختلفة للإجراءات المضادة المتوفرة للحد من بعض الثغرات المعروفة.

تتضمنُ أفضلُ الإجراءات المضادة نشاطات **الإدارة**، و**التنفيذ**، و**البنية** (MIC)(*) لتخفيف الثغرات ضمن شبكة (WLAN). يجب أن تطبق إجراءات الإدارة المضادة بالارتكاز على سياسة أمنِ معلوماتٍ مرسومةٍ رسماً متقناً. ينبغي أن تكون السياسةُ مرتكزةً على رؤيةٍ إداريةٍ وأن تقدِّمَ إطارَ عملٍ من أجل إدارة شبكة (WLAN). بعد ذلك ينفّذُ المدراءُ الرؤيةَ من خلال وضعهم محددات وقيم وضوابط الشبكة.

إجراءات مضادة إدارية

تعمل إجراءات الإدارة المضادة على تهيئة الساحة لكل ما يمكن أن يجري على شبكة (WLAN) بالارتكاز على السياسة، يجب أن تعمل هذه الإجراءات المضادة على:

ـ تعيينُ من الذي قد يستخدم تقنية (WLAN) في الشركة وتحديد النفاذ بحسب الوظيفة، والمكان، وفريق العمل، أو حسب الموافقات الأمنية.

ـ تحديدُ ما إذا كان الدخول إلى الإنترنت مطلوباً من خلال شبكة (WLAN)، فبعض تطبيقات (WLAN) تخدم الشبكات الداخلية فقط.

ـ توضيحُ من يسمح له بتنصيب نقاط النفاذ والأجهزة اللاسلكية الأخرى. إذ من الضروري التحقق من الاستخدام المناسب للتقنية نظراً إلى سهولة التنصيب.

ـ وضعُ تشديداتٍ حول مكان نقاط النفاذ وحول أمنها الفيزيائي لتقليل بثّ (مسافة وجاهزية) الإشارة.

(*) MIC = Management Implementation and Configuration.

ـ توضيح نوع المعلومات التي يسمح بأن ترسل عبر الروابط اللاسلكية لتقليل افتضاحات البيانات الحساسة.

ـ توضيحُ الظروف التي تُسمح فيها الأجهزة اللاسلكية.

ـ تحديدُ الأوضاع المعيارية لأمن المعلومات من أجل نقاط النفاذ لتقليل المخاطر وتعميم معايير موحدة للبنى.

ـ توضيحُ القيود حول كيفية استخدام الجهاز اللاسلكي مثل: الموقع ضمن أو خارج البناء، والقرب من المناطق الحساسة، لتجنب الوصول إلى البيانات الشخصية أو السِّرية.

ـ توضيحُ البنية المعتمدة البرمجيات والتجهيزات لجميع الأجهزة اللاسلكية.

ـ تزويد الإرشادات حول تقديم التقارير عند فقدان الأجهزة اللاسلكية وحوادث الأمن.

ـ تزويد الإرشادات من أجل حماية الحواسيب اللاسلكية لتقليل/تخفيف السرقة.

ـ تزويد الإرشادات حول استخدام أنظمة التعمية، وإدارة مفاتيحها.

ـ تحديد تواتر عملية تقييم الإجراءات الأمنية ونطاقها بحيث تتضمن موضوع اكتشاف نقطة النفاذ.

إجراءات مضادة عند تنفيذ الشبكة

إن إجراءات التنفيذ المضادة هي الضوابط في العملية. تعملُ الضوابطُ في إدارة شبكات (WLAN) على السماحِ بوقوعِ النشاط أو الحدث أو منعه. اعتَبِرْ جميعَ الشبكات اللاسلكية غير آمنةَ ومتوفرَة علانية. قُمْ بنقل نقطة النفاذ إلى «منطقة معزولة» (شبكة فرعية محمية على LAN) إذا أمكن، حيث تكون البيانات الحساسة غير متوفرة للمعتدين. ركّب جدران النار لتحميك من الاعتداءات ومحاولات الاعتداء.

ـ استخدم فقط نوع الحماية (WAPs) وبطاقة (NICs) التي تدعم تشفيراً قوياً أي على الأقل (WEP) ذي 64 خانة (ويفضل 128 خانة).

ـ خذ بعين الاعتبار استخدام أدوات تعمية، وكذلك أدوات التحقق من الهوية من جهة محايدة قبل أن تسمح بالاتصال بنقطة النفاذ إلى شبكتك.

ـ حاول انتقاء مكان نقطة النفاذ اللاسلكي (WAP) فيزيائياً بحيث تكون إشاراتها صعبة العثور بالنسبة إلى متلصصي الشبكة. أعط اهتماماً بالغاً لتوجيه الهوائي، وتجنّب تعيين مكان (WAP) بالقرب من النوافذ أو في غرفة قريبة من الشارع أو قريبة من موقف السيارات.

ـ قم بعملية تفحصٍ دورية للشبكات اللاسلكية ضمن مكان عملك/منزلك وحوله مستخدماً «متلصصاً» أو شركة استشارية متخصصة. إذ من السهل على أي موظفٍ شراء (NIC) و(WAP) وتنصيبهما على حاسوب من حواسيب الشركة. تقوم بعض أنظمة التشغيل بتجسيد (WAP) اتوماتيكياً مع الشبكة السلكية للشركة سامحةً بذلك النفاذ للشبكة (خلف جدار النار) والحصول على معلومات خاصة لأي شخص معه حاسوب محمول ببطاقة لاسلكية. ستحدد عملية التفحص ما إذا كانت إجراءات أمن المعلومات جاهزة أو ما إذا كان هناك أية تغييرات في بنية الشبكة. ستبين عملية التفحص أيضاً المسافة التي تصلها الإشارات اللاسلكية خارج بنائك.

ـ اشتر التقنيةَ اللاسلكيةَ ذات البرمجيات المخزنة بطريقةٍ لا يمكن تغييرها أو فقدانها والقابلة للتحديث. يجري تطويرُ تحسيناتٍ جديدةٍ في أمن المعلومات «كالنفاذ المحمي لـ (WAP) (Wi-Fi)»، ومع المنتج القابل للتحديث، فإن قدرتك على استخدام هذه التقنية تصبح أكبر. خذ بعين الاعتبار استخدام (WAP) التي أصبحت متوفرة. تمتلك WAP) العديدَ من المميزات الجديدة لأمن المعلومات اللاسلكية، بما فيها: التحقق من الهوية، وإدارة مفتاح التعمية، وبروتوكول سلامة المفتاح المؤقت (TKIP)، وتَفَحُّص سلامة وصول المعلومات، وحماية الردود، واحتواؤها على تعمية معيار التعمية المتقدمة (AES).

ـ اضمن أن حواسيبك تعمل وفق أحدث مستوى لرُقَع البرمجيات. إن هذا سيجعل مهاجمة أنظمتك ومعلوماتك أصعب إذا ما تمكن القراصنة من الوصول إلى الشبكة اللاسلكية.

ـ استخدم برنامجاً مضاداً للفيروسات والديدان مع آخر تحديثاته ضد الفيروس أو الدود الجديد. سيساعد هذا على منع المعتدي، الذي استطاع

دخول شبكتك، من تنصيب فيروس أو حصان طروادة للنفاذ سراً إلى حاسوبك، وسيحمي حاسوبك من برمجيات خبيثة أخرى.

ـ امنع الدخول فيزيائياً إلى مكان نقطة النفاذ، وأبقها بعيدةً عن الأنظارِ في مكان مقفلٍ، وبمنعك الدخول إلى (WAP) فإنك ستضمنُ عدمَ قيام أشخاص مدسوسين بإعادة تهيئة النظام، أو التحكم به، أو إعادة بناء الجهاز فيزيائياً.

إجراءات مضادة بنيوية

إن الإجراءاتِ المضادةَ البنيويةَ أسهلُ الإجراءات فهماً. تعالج هذه الإجراءات المضادة التحقُّقَ من الهوية، والتحكُّمَ بالدخول، وسلامةَ وصول البيانات، وسِّريةَ البيانات وأجهزة الحاسوب على الشبكة. إن إدراكَ كيفية بناء نقطة النفاذ هو أمرٌ هامٌ لتحقيق الرؤية الموضوعة في سياسة أمن منظمتك. ستخففُ البنيةُ المناسبةُ العديدَ من التهديدات وستحدُّ من الثغرات غير المتوقعة والمفاجئة. إن المقاربةَ الإيجابيةَ الفاعلةَ للموضوعِ هي أفضلُ وسيلةٍ لاتخاذ الإجراءات المضادة البنيوية؛ باعتبار أن كتيبات الإرشادات تأتي مع معظم التقنية اليوم، فمن المفروض أن يكون استنتاج أفضل بنية سهلاً من خلال قراءة هذه الكتيبات. إن من أهم المواصفات في هذا المجال ما يلي:

1. إستخدم «الخصوصية المكافئة للشبكات السلكية» أو «بروتوكول التعمية اللاسلكي» (WEP): يخفف هذا البروتوكول (WEP) من خطر اعتراض الإشارة الراديوية من قبل شخص ما قريب. صَمِّمْ (WEP) مع وظيفتي التعمية والتحقق من الهوية بين الحواسيب ونقاط النفاذ و(APs) وفقاً لمعيار (802.11b). تقوم حماية (WEP) على خوارزمية للتعمية تدعى (RC4). تقوم بعض المنتجات بالسماح بتعيين طريقة التحقق من الهوية لكلا النطاقين: النظام **المفتوح** أو نظام **المفتاح المشترك**. استخدم طريقة «المفتاح المشترك» لكي تستخدم التعمية للتحقق من هوية حاسوب زبائنك ولتشفير بياناته. وبالرغم من أن تعمية (WEP) قد كُسِرَتْ إلا أن استعماله لا يزال مربحاً بالنسبة إلى التكلفة (مجاني)، ويُعدُّ طبقةً أولى قيّمة للحماية. في بحثي طيلة السنين الثلاث المنصرمة، وجدت أن أكثر من 60٪ من نقاط النفاذ لا تستخدم (WEP)، بينما قد يسبب تفعيلُ هذه الخدمة انصرافَ المعتدي أو المستخدم الفضولي إلى هدفٍ أسهل. تُوَلِّدُ خوارزمية التعمية انطلاقاً من مفتاحٍ (تتابع الأرقام) مدخل ومُرَاقبٍ من قبل

المستخدم. تبنى جميع الحواسيب ونقاط النفاذ (APs) بمفتاح واحدٍ لتعمية وفك تعمية إرسال البيانات. إن مفاتيح (WEP) هي بطول 40 أو 128 خانة، وقد تبنى في ثلاث طرق ممكنة: طريقة عدم استخدام التعمية، أو طريقة التعمية بـ 40 خانه، أو طريقة التعمية بـ 128 خانة.

2. اجعل نقطةَ النفاذِ آمنةً بكلمة سر، يجب أن تطلب نقطة النفاذ إلى شبكتك كلمةَ سرٍ للدخول إلى مميزاتها الإدارية، إذا كانت لا تقوم بذلك استبدلها بواحدة تفعل. استخدم كلمات سر قوية لتحمي من أدوات اكتشاف كلمة السِّر. تأكد من أن نقطة النفاذ لا تستخدم كلمة السِّر الموجودة في الأصل عند شرائك للجهاز (default). إن كلمة السِّر الموجودة في الأصل معروفة، وستكون واحدة من أولى الاستغلالات التي سيجربها المعتدي المتمرس. يحدِّدُ العديدُ من أجهزةِ الكشفِ اللاسلكيةِ الصانعَ انطلاقاً من «عنوان التحكم بالنفاذ إلى الوسائط» المخزن في بطاقة الولوج إلى نقطة النفاذ (MAC of the AP)، إن هذه المعلومات تُسَهِّلُ تخمينَ نوع (WAP) المستخدم، حتى لو تم «تغيير مُعَرِّف مجموعة الخدمة» (SSID). قم بتغيير كلمة السِّر بشكل دوري.

3. غيِّرْ معرف مجموعة الخدمة SSID) إلى اسم استثنائي فعلاً بحيث لا يشير إلى مالك نقطة النفاذ. يسمح (SSID) لشبكة (WLAN) أن تكون مفصولة إلى شبكات عديدة، ولكل شبكة معرِّفٌ مختلف. تُعطى كلُّ شبكةٍ من هذه الشبكات معرّفاً مختلفاً يُبرمج لواحدة أو أكثر من نقاط النفاذ (APs). للدخول إلى أي من هذه الشبكات، على حاسوب المستخدم أن يتمتع بالمعرِّف المطابق (SSID) لتلك الشبكة، وبالتالي يعمل المعرف (SSID) ككلمة سر بسيطة تزود درجة من الحماية. تُخلقُ نقطة الضعفِ عندما يُعْرَفْ (SSID) أو تتم مشاركته، أو يكونُ الحصولُ عليه سهلاً بوساطة برمجياتٍ مجانيةٍ محملةٍ على حاسوب المستخدم للشبكة اللاسلكية.

4. قم بتعطيلِ بثِّ «مُعرّف مجموعة الخدمة (SSID)» إذا كانت هذه الميزة متاحة من قبل بائع الأجهزة. إن معظم نقاط النفاذ تبثُّ المعرف (SSID) حكماً (default). إن هذا يجعلُ الشبكةَ تقبل أي (SSID). بتعطيل بثِّ المعرفِ (SSID)، يتحتم تطابق معرِّف الخدمة المبرمج في حاسوب المستخدم مع معرِّفِ نقطة النفاذ.

5. أغلق بروتوكول تكوين الحاسوب المضيف ديناميكياً (DHCP)، وعيِّنْ

عنوانَ بروتوكول إنترنت (IP) ثابت للأجهزة اللاسلكية. سيجعل هذا (WAP) خاصتك يمتنع عن إرسال عنوان (IP) إلى أي حاسوب يحاول الاتصال به. خذ بعين الاعتبار أيضاً تغيير (IP) الشبكة الفرعية إلى عنوان غير العنوان الأصلي default. إن العديد من نقاط النفاذ تعتمد الـ IP ذا الرقم (192.168.1.0) للشبكة، وتستخدم الـ IP ذا الرقم (192.168.1.1) كعنوان أصلي (default) للموجِّهِ (Router). يزودُ تغييرُ هذه الأمور الموجودة في الأصل (defaults) طبقات إضافية للحماية.

6. قم بترشيح الأجهزة وفق عناوينها المجسدة فيها (MAC). يزيد الترشيح من أمن المعلومات من خلال تزويد نقطة النفاذ بقائمةٍ بعناوين (MAC) للحواسيب التي يسمح لها بالدخول إلى نقطة النفاذ. إذا كان عنوان (MAC) للحاسوب المستخدم غير موجود على القائمة، فإن نقطة النفاذ ستمنع دخوله. تُقدمُ هذه الطريقة أمن معلومات جيداً، ولكنها تلائم الشبكات الصغيرة فقط. من الواضح أن العمل الكبير اللازم لإدخال عناوين (MAC) وإبقاء القوائم محيَّنة أو محدَّثة لجميع أجهزة نقاط النفاذ يخفف من جدوى هذه الطريقة. قد تُركَّبُ نقطةُ النفاذ مع حماية التعمية فقط في طريقة النظام **المفتوح**، أو تضيف تَعَرُّفَ الهوية في طريقة **المفتاح المشترك**. يُستخدمُ غالباً ترشيحُ عنوان (MAC) مع هذه التعمية. إن حماية (WEP) تلائم الشبكات الصغيرة نظراً إلى عدم وجود بروتوكول لإدارة المفاتيح. وبالنتيجة، يجب أن تُدخَل المفاتيح يدوياً إلى كلِّ حاسوب. قد يشكل هذا عبئاً إدارياً هائلاً، خاصة أنه ينبغي تغيير المفاتيح بشكل منتظم لتزويد مستوى حماية أعلى.

قم بتطويل مدة «منارة» نقطة النفاذ (الفترة الزمنية الفاصلة بين بَثَّيْنِ لِمُعَرِّفِ الشبكة). إذ تعلنُ معلوماتُ المنارةِ عن وجودِ شبكتكَ اللاسلكيةِ إلى الجميع. تُرْسَلُ هذه المنارات من قبل نقاط النفاذ في أوقات زمنية منتظمة وتسمح لمحطة حاسوب المستخدم بتحديد وملاءمة بنيته لكي تتصل بالشبكة اللاسلكية. من المناسب وضع المدة على قيمتها العليا وهي 67 ثانية تقريباً.

كطريقة أكثر أمناً، طَوَّرَ بعضُ البائعين حلولَ شبكة افتراضية خاصة (VPN) التي تُقيمُ نفقاً آمناً من أجل حركة المرور اللاسلكية الخاصة بك. تتضمن منتجات الحماية اللاسلكية المطورة الآن وسائل للتحقق من هوية جميع المستخدمين اللاسلكيين قبل أن يتمكنوا من الدخول إلى مصادر الشبكة، ولتعمية البيانات قبل

بثّها على الهواء مستخدمةً معيار التعمية المتقدم (AES)، ومُتَحكِّمةً بدخول المستخدم إلى أجزاء الشبكة من خلال استخدام «مخدمي السياسة».

ماذا بعد؟

يعمل العديد من الأشخاص من أجل تحسين أمن شبكات (WLAN)، والهدف من ذلك في المقام الأول هو رفع جودة وظيفة أمن الشبكة، أما الهدف في المقام الثاني، ولكنه بنفس درجة الأهمية، فهو تعزيز ثقة مستخدمي ومدراء الشبكات اللاسلكية. ثمة ثلاث طرق لديها بوادر نجاح تُوَطِّدُ مستقبل شبكات 802.11 (WLAN)، وهي:

(nDosa)

قد يُدعم مستقبل الشبكات اللاسلكية الآمنة (WLAN) بمنتجات مثل نقطة النفاذ المسماة (nDosa). أَدخَلَت تقنيات (nDosa) تقنية (LAN) اللاسلكية الآمنة التي تعتمد على خوارزمية أمن (nESA) (خوارزمية الحماية المعززة) nDosa، التي تجعل إشاراتها غير مرئية للقراصنة وللمراقبين غير المسموح لهم، وبالتالي تقلل كثيراً من قابليتها للقرصنة والانتهاك. ولكن يجب التنويه إلى أن بعض القراصنة المصممين لا يزالون قادرين على مراقبة الإشارة الراديوية (RF) ورصد نشاط شبكة (LAN) عبر الهواء، إلا أن اقتحام النظام من قبلهم سيكون أمراً بمنتهى الصعوبة (Kim and Shin, 2003). إن هذا الحل مثله مثل حلول (WLAN) الأخرى فهي جميعها: قابلة للتوسعة أو التصغير، وقابلة للتحسين، ومرنة، ومن الممكن تعديلها وفقاً لطلب الزبون.

يستطيعُ مستخدمو شبكاتِ (WLAN) الآمنةِ (nDosa) ليس فقط الدخول إليها، وإنما إلى كل شبكات (WLANs) المعيارية أيضاً والمنتشرة بشكل واسع في الأمكنة العامة أو في المناطق المحمية حماية عالية. عندما تقتضي الضرورة تعزيز التحقق من الهوية، أو إجراء إدارة المفتاح، فإن تقنية (WLAN) الآمنة (nDosa) تعتبر الحل بدون منازع. إن خوارزميات التعمية وحلول الأمن تتطلب التحسين باستمرار لأنها في صراع دائم مع القراصنة. ووفقاً لما هو منشور فإن خوارزمية (nESA) قد صممت لجعل التحسينات بسيطة وسهلة.

إن الجمعَ بين مخطط (LAN) اللاسلكية المقترح مع تقنية (LAN) اللاسلكية الآمنة (nDosa) سيجعل النظام ليس فقط غير مرئي، حتى في الحزمة

الراديوية (RF)، وإنما سيضمن أيضاً أن النظام سيبقى منيعاً نسبياً للهجمات حتى لو تم اكتشاف الإشارة. إن تطبيق إجراءي الأمن المذكورين كليهما، سيزوّد شبكة (LAN) اللاسلكية بحماية قوية جداً صالحة وملائمة لصون بيانات وبرامج الحكومة.

النفاذ المحمي للـ Wi-Fi (WPA)

إن «النفاذ المحمي للـ (Wi-Fi)» هو مواصفة لمعيار تحسين أمن المعلومات المتبادلة لاسلكياً، وهي تزيدُ زيادةً كبيرةً مستوى حماية البيانات ومستوى التحكم بالنفاذ في أنظمة الشبكات (LAN) اللاسلكية الموجودة والمقبلة. إن «النفاذ المحمي للـ (Wi-Fi)» قد صمم للعمل على أجهزة الحاسوب الحالية كتحسينٍ برمجيٍ مشتقٍ من ومتلائمٍ مع معيار (802.11i IEEE)[1].

إن المعيار (WPA) هو تجاوب إيجابي من قبل الصناعة بتقديم حلٍّ قويٍ وفوريٍ لأمن المعلومات. تتوفرُ الآنَ برمجيات تحسينية ورخيصة للتَنصيب في الشبكاتِ المحلية اللاسلكية للمؤسسات أو للمنازل/المكاتب (SOHO). إن هذا الحل هو حلٌ مُوَحَّدٌ من قبل العديد من البائعين وهو قابلٌ للتركيبِ على المخدمات التي تَتَطلَّبُ التحقق من الهوية أو على حاسوبٍ مستقل. إن معيار (WAP) هو فرعٌ للمعيار (802.11i) وسيبقي قادراً على الملاءمة المستقبلية.

لقد تمَّ وضعُ مُواصفةِ النفاذ المحمي لـ (Wi-Fi) لتقدمَ تعميةً محسنةً للبيانات التي كانت ضعيفة في (WEP)، ولتوفرَ عملية التحقق من هوية المستخدم المفقودة غالباً في معيار (WEP). تركزُ هذه التحسينات على استخدام التعمية المعززة للبيانات من خلال بروتوكول سلامة المفتاح المؤقت (TKIP). يزود بروتوكول (TKIP) تعزيزات مهمة لتعمية المعلومات، بما في ذلك وظيفة خلط المفتاح قبل كل عبوة Pre-Packet وتفحص سلامة معلومات الرسالة Message Integrity Check (MIC) المسمّى ميشال (Michael)، والموجّه الابتدائي الممتد Initialization Vector (IV) مع قواعد تسلسل، وآلية إعادة إدخال المفتاح. يعالج (TKIP) من خلال هذه التعزيزات جميع ثغرات (WEP) المعروفة.

(1) <http://www.wi-fi.org/OpenSection/pdf/wi-fi_protected_Access_overview.pdf>.

جدول مقارنة

	WEP	WPA	802.11 i	nDOSA
التعمية	RC4	RC4	CTR-CCMP	nESA
حجم المفتاح	40 خانة	تعمية 128 أو 64 خانة، تحقق من الهوية	128 خانة	256˜128 خانة
حياة المفتاح	48IV ـ خانة	48IV ـ خانة	48IV ـ خانة	48IV ـ خانة
مفتاح العبوة (كتلة معلومات)	متسلسل	وظيفة خلط	غير لازمة	وظيفة خلط
سلامة وصول البيانات	CRC ـ 32	ميشال	CCM	CRC ـ 32
سلامة وصول الترويسة (header)	لا يوجد	ميشال	CCM	nESA
الاعتداء المعتاد	لا يوجد	سلسلة IV	سلسلة IV	IV معماة
إدارة المفتاح	لا يوجد	EAP	EAP	EAP وطرق أخرى
تعمية الترويسة (header)	لا يوجد	لا يوجد	لا يوجد	nESA
الطريقة المخبأة	لا يوجد	لا يوجد	لا يوجد	نعم

إن استخدامَ معيار التحقُّقِ من هوية المستخدم لمستوى المؤسسة (802.1X) «وبروتوكول التحقق من الهوية الموسع» (EAP) يقوي عملية التحقق من الهوية.

إن مواصفة (WEP) لا تمتلك تقنية للتحقق من هوية المستخدم. تَسْتَعْمِلُ مواصفةُ «النفاذ المحمي للـ Wi-Fi» المعيارَ 802.1X وبروتوكول (EAP).

تُشَكِّلُ هذه الأدواتُ مجتمعةً إطارَ عملٍ قوي من أجل التحقق من هوية المستخدم. يَستَخدِمُ إطارُ العملِ هذا خادماً مركزياً للتحقق من الهوية، مثل (RADIUS) وذلك للتحقق من هوية كل مستخدم على الشبكة قبل اتصاله بها، ويوظفُ أيضاً «التحقق المتبادل» لكي لا يتصل المستخدمُ اللاسلكيُ عَرَضاً بشبكة خبيثة قد تسرق المعلومات المعتمدة لشبكته.

حلول دفاعية للمؤسسة

لقد طورت العديدُ من الشركاتِ حلولاً لشبكات (WLAN) خصيصاً للمؤسسات، بحيث تعالج العديد من الثغرات المتعلقة بـ (802.11b). تتطلب حاجات المؤسسة عادةً عدَّةَ مستويات من الدفاع. يجب على مدراء شبكة (WLAN) في أي مؤسسة أن يمتلكوا مجموعة من البرمجيات التي تلبّي الحد الأدنى لمعيار هيكلية أمن المعلومات. ينبغي أن يتضمن الحل على الأقل ما يلي:

ـ تحققٌ من الهويةِ متبادلٌ بين المستخدمين والشبكة.

ـ التَّحكمُ بالدخول إلى نقاط النفاذ والموارد الموجودة على الشبكة السلكية.

ـ تحكمٌ بالنفاذِ مبنيٌ على اللائحة.

ـ استعمال الترخيص للمستخدمين والأجهزة.

ـ سِّرية الرسالة.

ـ التحقق من هوية الرسالة.

ـ الإدارة الديناميكية لمفتاح التعمية.

ـ عزل حركة المرور اللاسلكية عن شبكة (LAN) السلكية.

ـ بروتوكول تعمية (التشفير) عالي المستوى.

إن «الجدار اللاسلكي» المطور من قبل شركة Cranite System Inc. هو حلٌ شاملٌ للشبكة اللاسلكية للمؤسسات (WLAN)، فالجدار اللاسلكي(2) هو مجموعة من البرمجيات التي تتعامل مع حالة البنية **المفتوحة**. هذا الحل مصممٌ لإدارة وأمن الشبكات اللاسلكية التي تسمح بأكبر حرية ممكنه لحركة المستخدمين. يعملُ «الجدار اللاسلكي» على نحوٍ متبادل مع تطبيقات الحماية والإدارة والسياسة الموجودة، ويزود دعماً كبيراً لمجموعة متنوعة من الأجهزة اللاسلكية.

---

(2) <http://www.cranite.com/pdf/whitpapers/wirelesswall-tech-op.pdf>.

إجراءات المتابعة

ينبغي أن تشتمل سياسات أمن المعلومات للمنظمة على تقييم وتفتيشٍ دائمين لهذا الأمن، وهذه هي الطريقة المثلى لقياس نجاح خطة أمن شبكة (WLAN). تعدُّ عمليةُ التقييم حجرَ الأساسِ في تحديد الحالة الراهنة لأمن المعلومات، وذلك من خلال تقييم البنية مقارنةً بالممارساتِ الأفضل ومعاييرِ الصناعةِ المعترفِ بها.

إن عمليةَ التقييم هي أداةٌ إداريةٌ ممتازةٌ تحددُ نقاطَ الضعف ونقاط القوة في أمن المعلومات. تُستخدمُ نتائجُ التقييم بعد ذلك للسماح للإدارة بترتيب أولويات الموارد والجهود من أجل المستقبل. إن عمليةَ التقييم أساسيةٌ لتفحُّصِ وضعية أمن شبكات (WLAN) وتحديدِ الإجراء الإصلاحي اللازم للتأكد من بقائها آمنة. أما التفتيشُ فيراقب الضوابطَ الحاكمةَ للشبكة اللاسلكية (WLAN) تبعاً لما هو مذكور في الوثائق. يقوم المدققون بتفحُّصِ الوثائق، ويُجرونَ مقابلاتٍ مع المستخدمين ويبحثونَ في الاتجاهاتِ المستقبليةِ لتقرير ما يُفترضُ أن تقوم به خطط الأمن. إذا وُجِدَ أنَّ الضوابطَ المكتوبةَ هي نفسها في التطبيق، فإن التدقيق يبشر خيراً.

أما إذا كانت هناك فجوةٌ بين النشاطات المكتوبةِ وتلك المنفَّذَةِ فإن التفتيش يعتبر غير مرضٍ. إنه أمر مهم للشركات أن تقوم بعمليات تفتيشٍ منتظمةٍ باستخدام محللي الشبكة اللاسلكية وأدواتٍ أخرى. إن المحلل وهو ما يدعى أحياناً بـ «المكتشف أو المشمشم» هو أداة فعالة لإدارة عملية التفتيش على أمن المعلومات وإصلاح خللِ الشبكة اللاسلكية (Karygiannis and Owens, 2002). قد يَسْتَخْدِمُ مدراءُ الأمن أو مفتشوه محللي الشبكة لتحديدِ ما إذا كانت المنتجات اللاسلكية المشتراة تُرْسِلُ إشاراتها بشكلٍ صحيح وعلى القنوات الراديوية الصحيحة. يتوجب على المدراء أن يتفحصوا بشكلٍ دوري داخل بناء الشركة وفي حَرَمِها نقاطَ النفاذ الخبيثة طرقَ النفاذ المحظور الأخرى.

قد تفكرُ الوكالاتُ الحكومية أيضاً باستخدام طرفٍ ثالثٍ مستقلٍ لإدارة عمليات تفتيش أمن المعلومات. إن مستشاري الطرف الثالث المستقل هم غالباً أكثرُ عصريةً بشأن الثغرات الأمنية، وهم مدربون بشكل أفضل فيما يخص حلول أمن المعلومات، ومجهزون بما يلزم لتفحص حماية الشبكة اللاسلكية وتقييمها.

سيساعد التفتيش من قبل الطرف الثالث المستقل، الذي قد يتضمن اختبار اختراق الوكالة، في التأكد من أن شبكة (WLAN) خاضعة لإجراءات وسياسات الأمن المعتمدة، وأن النظامَ متطورٌ بشكل يتلاءم مع تحسينات وتحديثات ورقع البرمجيات الأخيرة.

استنتاجات

إن كلاًّ من الأجهزة اللاسلكية، وشبكات (WLAN) والثغرات هي هنا لتبقى. تُبْتَكَرُ تطبيقاتٌ جديدةٌ أكثر فأكثر مستخدمةً التقنية اللاسلكية وتنتشرُ عبر السوق. سيتزايدُ الطلبُ على شبكات (WLAN) في السنوات المقبلة، مع جهودنا في جعل جميع هذه الأجهزة الجديدة تعمل بسهولةٍ تامةٍ لخدمةِ المؤسسات. وكلما كانت المنظمات أسرع في تعميم التحديات المتعلقة بشبكات (WLANs)، كان أمنها أقوى. إن بعضاً من الثغرات والتهديدات هي نفسها لدى الجميع لأن البائعين يطبقون معيار (802.11b) بدون إجراء تغييرات لخدمات الأمن، فالمشكلات التاريخية والموثقة جيداً هي نفسها من جهاز إلى جهاز، وهو أمر جيد للمستهلك والبائع ولكنه مشكلة لمالكي شبكة (WLAN) الجدد لعدم خبرتهم بها.

تخطيط تقادم البيانات وإدارته

ستواجه المنظماتُ التي تمتلكُ أو تستخدمُ قواعدَ بياناتٍ ضخمة ومستودعاتِ معلومات، نفقةً كبيرةً في الثلاث إلى السنوات العشر المقبلة نظراً إلى أن بيانات التعاملات التجاريةِ السابقة قد أصبحت قديمة وتقتضي التقاعد بعيداً عن التداول اليومي أو عن أنظمة الإنتاج. إذا ما أخذنا بعين الاعتبار سرعة تولد المعلومات الجديدة ـ وبالرغم من تقنيات تخزين المعلومات الجديدة اللافتة للنظر التي تبدو أنها تستحدث كميات غير محددة من السعة ـ فمن المنطق في نقطة ما من الزمن أن تزاح المعلومات التي عمرها خمس، أو 10 أو 20 سنة باعتبار أن قيمتها منخفضة.

من وجهة نظر أمن المعلومات، تُقلِّلُ المعلوماتُ التي تُزاح أو تُزال من منظومة الشبكة، احتمالَ النفاذِ المحظور لمعلومات تلك المنظومة، ولكنها تخلق فرصاً جديدة للسرقة، أو الضياع، أو الأذى ولكن بطرقٍ أخرى. إن ابتداعَ

عمليةٍ رسميةٍ مع إجراءات عديدة لتأكيد أمن المعلومات، بما في ذلك نظام رقابة وتفتيش هي عناصر هامة لضمان أمن المعلومات.

على سبيل المثال، إن المعلومات التي تكون في حيازة البنك حول حساباتٍ قد أغلقت منذ 15 سنة مضت، قد تُزالُ كلياً من التداول وتُخَزَّنُ بعيداً عن الموقع في مكان آمن. وإذا اقتضت الحاجة إليها ـ ربما في تحقيقات ضريبة أو دعوى قضائية ـ فسيكون من الممكن استرجاعها واستعمالها، ولكن ربما لن يكون هذا ممكناً إذا كان خزنها غير مدروس.

فمثلاً، إذا ضاع **فهرس** الملفات الرئيسي أو خُرِّبَ، فإن البنك قد لا يعلم أين يبحث عن الملف في الأرشيف. أو لنفترض أن الفهرسَ صالحٌ للاستعمال إلا أن **وسائط التخزين**، مثل الشريط المغناطيسي أو (CD-ROM) أو القرص المغناطيسي، التي تحتوي على الملفِّ قد أُزيلت من مرفق التخزين. حتى أسوأ من ذلك، من المحتملِ أن يكون الملف قد نسخ من قبل مستخدمين غير مخولين بذلك، ومن ثم أعيد إلى مرفق التخزين بدون أن يلاحظ ذلك أحد. لقد نُقِلَتِ المخاطرُ إذاً من نظامِ الإنتاج إلى نظام الأرشيف.

كذلك، ماذا عن **بنى** الملفَّاتِ البرمجيةِ أو الماديةِ التي تتغير مع التقدم السريع للتطورات التقنية؟ ففي عام 1980، كانت سعة خزن الشريط المغناطيسي عالي الكثافة 6250 خانة في كل أينش من طول الشريط. تُخَزِّنُ اليومَ الأشرطةُ المغناطيسيةُ المخصصةُ لحفظ البيانات 100 مرَّة تلك الكثافة، وبعدَ سنواتٍ قليلةٍ ستتجاوز الـ 1000 مرَّة. هل يُمكن استعادة البيانات التي خُزِّنَتْ على بنية 6250 وخزنها من جديد على بنية جديدة؟ نعم، ولكن بنفقة ضخمة تقع على المنظمة التي تحتاج هذا التحويل. إذ تُستَبدَلُ غالباً تجهيزات الحاسوب المتقادمة تقنياً بأنظمةٍ جديدةٍ لا تتوافق مع أنواع وسائط التخزين والبنى البرمجية القديمة. قد يكون تحويل القليل من الأشرطة أو الملفات ممكناً، عن طريق التعاقد مع شركة يستعان بها في ذلك، ولكن ماذا لو كُنتَ تمتلك 50,000 شريط أو قرص ليزري (CD-ROMs)؟ ماذا لو أنك لم تعرف أيّاً منها يحتوي البيانات التي تبحث عنها؟ فيما يتعلق بالشركة الضخمة جداً التي تمتلك العديد من «التيرا بايت» من المعلومات القديمة، فإن التكلفة قد تتجاوز مئات ألوف الدولارات لتحديث فهارس التخزين، وتحديث الأشرطة، و(CD-ROM)، وأجهزة ذاكرة (USB) بشكل مستمر لضمان الملاءمة مع البنى والأجهزة الحديثة.

هناك عدد من المفاهيم الواجب استحضارها في الذهن دائماً عند التعامل مع أمن المعلومات المتقادمة:

1. عَيِّنْ «أعماراً « أو «حياةً» لاستخدام المعلومات، وقُمْ بحفظِ (أرشفة) المعلومات غير الضرورية بشكلٍ دوري.

2. استخدم نظاماً منطقياً لفهرس المحفوظات (الأرشيف) لجميع الملفات يُحَدِّدُ بسهولةٍ مكانَ الملفِّ أو مجموعة الملفات، حتى لو فُقِدَ الفهرس الرئيسي أو خُرِّب.

3. اضمن أن لا يقوم نفس الأشخاص بعمليات النسخ، والفهرسة، والحفظ، والتحقق، بل عدَّة أشخاص كي يَتفحَّصَ كلٌّ واحد منهم عَمَلَ الآخر.

4. قم بتأدية مراقبة عملية حفظ المعلومات المتقادمة والتفتيش عليها من خلال تجربة إمكانية استعادة البيانات المحفوظة (المؤرشفة) إلى بنى وأجهزة جديدة.

5. اضمن أمن مواقع المحفوظات البعيدة عن نظام الإنتاج ـ استخدم موقعين اثنين على الأقل لضمان احتمال المحافظة على المعلومات ـ من خلال اختبارات وتدقيقات من قبل طرف ثالث.

6. عند تحديث التجهيزات الحاسوبية (شريط مغناطيسي أو قرص التخزين)، حاول الحصول على أقصى ضمانات الملاءمة الارتجاعية الممكنة، لتقليل التكلفة والجهد اللازمين لتحديث معلومات المحفوظات القديمة.

تخطيط وإدارة بروتوكولات البيانات الاحتياطية واسترجاعها

بينما يبدو الأمرُ بسيطاً من حيث الفكرة، إلا أن حفظَ وصيانةَ كمياتٍ كبيرةٍ من المعلومات كنسخةٍ احتياطيةٍ كل يوم (أكثر من خمسة غيغا بايت يومياً) يتطلب بروتوكولات تكرار وعملية مهمة لضمان قدرة الأنظمة على العمل عند وقوع حوادث غير متوقعة. إن عمليات استعادة المعلومات ضرورية عندما تصاب تجهيزات الحاسوب بخلل كهربائي أو ميكانيكي خطير، أو حينما تقع حوادث بيئية (مثل حادث انفجار أنابيب مياه إطفاء الحريق مغرقةً بذلك

غرفة الحاسوب) أو عندما تُشَنُّ اعتداءاتٌ خبيثةٌ ضد المنظمة ومنشآتها.

إن حفظَ نسخةٍ احتياطيةٍ عن معلوماتِ نظامٍ يعملُ (7×24) بدونَ توقفٍ يجب أن يُدرج ضمن خطةٍ تأخذُ بالاعتبار أنَّ بعضاً من البيانات لا يمكنُ حفظها بسببِ الطبيعةِ المغلقةِ لقواعدِ البياناتِ العلائقية التي تمنعُ النَّسْخَ أثناءَ العمل. كذلك قد تؤثر عملية حفظ نسخة احتياطية من البيانات يومياً في أداء النظام، وبالتالي في إنتاجية المستخدم ورضا الزبون.

يعتمد تعقيد عملية الاسترجاع على كمية المعلومات التي تُسترجَع: هل الذي يقتضي الاسترجاع ملفٌ واحدٌ، أو سواقةُ قرصٍ واحدة، أو نظامٌ واحد، أو أن كلَّ شيء يستدعي ذلك؟ هل تغطي فترةُ الاستعادة يوماً واحداً، أو أسبوعاً أو شهراً؟ أو أكثر؟ هل من الضروري جلب أشرطة أو أقراص حفظ البيانات إلى غرفة الحاسوب، أو أنها موجودة داخل الغرفة؟ هل هناك من يعلم أين حفظت الملفات الاحتياطية، وما هي تلك الملفات، وعلى أيٍّ من وسائل التخزين؟

يصبح موضوعُ حفظ البيانات واسترجاعها موضعَ اهتمام الإدارة بعد تمويلها ميزانيات ضخمة لتقنية المعلومات ولعدة سنوات، أو عندما لم يعد ممكناً استرجاع البيانات بسبب أعطال في الأجهزة، أو عندما تُفقَدُ أو تَنقُصُ بعض الملفات أو البيانات من وسائط تخزين المعلومات الاحتياطية أو المحفوظات، أو عند إخفاق الأعمال التجارية. من وجهة نظر أمن المعلومات إن عدم القدرة على استعادة المعلومات عند الحاجة إليها ـ مهما كان السبب ـ يضع المنظمة موضع خطر كبير نظراً إلى الأثر المالي أو فشل العمل.

ما الذي يتوجب فعله لتقليل مخاطر فقدان البيانات وأثارها في العمل بسبب رداءة عمليتي الاسترجاع وحفظ البيانات؟ من الممكن إتباع طرق عديدة منها:

1. استَخْدِمْ قاعدةَ النسبتين المئويتين (20 ـ 80) كي تُحَدِّد ما الذي يتوجب حفظه يومياً (أو في كل ساعة) وما الذي يَحْتَمِلُ الانتظارَ فترةً أطول.
2. اختَبِرْ أنظمةَ الأشرطة المغناطيسية والأقراص الليزرية أسبوعياً لاكتشاف أي أعطال أو أي وثوقية غير نظامية.
3. اختبر كلَّ نسخ البيانات المحفوظة على أنظمة قراءة مختلفة لضمان إمكانية قراءتها في أي نظام، وليس فقط النظام الذي كتب الملفات.

4. ضع لصاقة واضحة على كل وسيلة تخزين، مستخدمة لحفظ البيانات، مع فهرس بأسماء الملف وأنواعه.

5. احفظ جميع وسائل التخزين المستخدمة لحفظ البيانات في مكان آمن ومحمي، بعيداً عن التحريف، أو السرقة أو التلف العرضي.

6. حضّر نسخاً عديدة من الفهارس، واحفظها في أماكن أو خزائن مختلفة آمنة.

7. اجعل صانعي الأجهزة يتحققون كل ستة أشهر من أن معداتهم تعمل، ووسائط التخزين تُستخدم بشكل صحيح، وأن عمليات الاستعادة ناجحة.

8. من وجهة نظر أمن المعلومات، اضمن أن عمليات النظام لن تُعاق بسبب فقدان البيانات أو فقدان سعة المعالجة الناتجة من اعتداءات أو انتهاكات أمنية.

استخدام المؤثرات البيولوجية

يشير قياس المؤثرات البيولوجية إلى التقنيات التي تميز أعضاء الجسم البشري وتتحقق منها أو من خصائصها أو عملها. تتضمن هذه التقنيات قارئات بصمة الإصبع، وفاحصات الوجه، والفاحصات الشبكية، وقارئات بصمة الصوت، والتوقيع. تعمل هذه التقنيات على مقارنة النموذج الرقمي المزوَّد من قبل المستخدم والتحقق منه أوتوماتيكياً مقارنةً بقاعدة بيانات الهويات «المعروفة». إذا كان هناك تطابقٌ، فإن المستخدم يُعترف به و«تُثبَّت هويته»، أما إذا لم يكن هناك تطابقٌ، فإن النظام يحفظ المعلومات الرقمية من أجل المعالجة الإضافية لتحديد من هو ذلك المستخدم.

لقد كانت تقنية استخدام المؤثرات البيولوجية في حافة القبول لسنوات عديدة، إلا أن التكاليف المرتفعة والتساؤلات حول وثوقيتها قد قيّدت انتشارها تجارياً على نطاق واسع. أثناء السنوات الخمس الأخيرة تمّت معالجة هذه المواضيع من خلال التحسينات التقنية للايجابيات الخاطئة (تمييز شخصٍ على أنه شخص آخر خطأً)، وعمليات الرفض الخاطئة (رفض الشخص الصحيح خطأً)، وبالتالي أصبحت هذه التقنية الآن تتمتع بنسبة نجاح مقبولة تساوي 99.9٪ المطلوبة من أجل التطبيق التجاري.

تعتبرُ طرقُ الحماية البيولوجية واحدةً من أكثر طرقِ التعرُّف أمناً، باعتبارها تتحققُ من أمرٍ تقوم به أو من أمرٍ هو جزءٌ منك. على سبيل المثال، إن توقيعك وطريقة ضربك على الحاسوب هو أمرٌ تقوم به، أما بصمة إصبعك أو معالم وجهك أو صوتك أو شبكية عينك، فهي جزء منك. إن أجهزةَ التحقق من المؤشرات البيولوجية أفضلُ بكثير في حماية الدخول من كلمات المرور أو الوسائل الفيزيائية مثل المفاتيح والإشارات لكونها أكثر صعوبة في السرقة أو المشاركة.

تعطي التقنياتُ البيولوجية، عندما تُدمجُ مع طرقِ تعرُّفٍ أخرى، حمايةً قويةً من الدخول المحظور إلى المعلومات والأنظمة والشبكات.

يصنف عادة قياس المؤشرات البيولوجية إلى أربعة مجالات:

1. **العمومية**: يجب أن يكون استخدام النظام ممكناً من قبل جميع الأشخاص.

2. **التفرد**: يجب أن لا يملك شخص آخر الميزة ذاتها.

3. **الاستمرار**: يجب أن تكون الميزة ثابتة عبر الوقت.

4. **قابلية القياس**: يجب أن تكون الميزة قابلة للقياس كمياً.

يتفحص مزودو النظام، عند انتقاء الطريقة البيولوجية للتحقق من الهوية، أداء الجهاز (السرعة، والدقة، والوثوقية) ومدى حيازته لقبول المستخدمين (هل هو مؤذٍ أو خطير أو مهين) والمراوغة الممكنة عليه (إلى أي درجة يستطيع المستخدمون خداع النظام). بغضّ النظر عن نوع الجهاز، فإن عملية التثبت من الهوية تعمل بنفس الطريقة وهي:

تؤخذ عيّنةٌ من الميزة البيولوجية للشخص وتحولُ إلى رموز حسابية تستخدم في «المطابقة» لاحقاً. عندما يرغبُ المستخدمُ بالدخول إلى النظام تُؤخَذُ عيِّنةٌ جديدةٌ ـ مثل بصمة الإصبع ـ وتقارن بالعينة السابقة، إذا تطابقت يُسمحُ للمستخدم بالدخول، وإذا لم يحصل التطابق فإنه قد يُسأل سؤالاً صعباً، أو قد يُطلب منه تقديم عيّنة أخرى للتحقق من هويتهِ، إذا فشل التطابق الثاني يمنع من الدخول.

أين ينبغي استخدام التقنية البيولوجية؟ بالرغم من أنها قد تستخدم أينما

كان، إلا أن أكثرَ الأماكن فائدةً بالنسبة إلى التكلفة هي حيث يجب التثبت من هوية المستخدم بشكلٍ جازم. من الأمثلة: صرف الصيدلي لوصفة طبية حساسة، أو التاجر المالي المُعْتَمَدُ لنقل ملايين الدولارات في التجارة كلَّ يوم، أو الأشخاص ذوو الحاجة إلى التحقق من التصاريح الأمنية، أو السجناء المدانون الذين قد يملكون اسماً أو مظهراً مرئياً مشابهاً لشخص آخر لمنعهم من مغادرة السجن بدلاً منهم.

أما في عالم تقنية المعلومات فتتضمن تطبيقات الأمن النموذجية التحكم في الدخول إلى منشآت وغرف الحاسوب، والنفاذ إلى أنظمة الحاسوب وشبكاته، وكطريقة لكتابة الاسم والتوقيع للمستخدمين الذين يستخدمون أنظمة متعددة مع طريقة واحدة للتثبت من الهوية.

البطاقات الذكية

إن البطاقات الذكية هي أجهزة نفاذ بحجم بطاقة الائتمان، وتستخدم كأداة ذاكرة قابلة للحمل والمحي، وهي معروفة بأسماء مختلفة. يمكن استعمال البطاقة الذكية مع كلمة السِّر ومع المؤشرات البيولوجية، وقد تحتوي البطاقة الذكية على خوارزميات تعمية، أو صفات مميزة بيولوجية، أو سيرة الشخص الصحية، أو عمليات الشراء السابقة له، أو معلومات أخرى تعزِّزُ أمكانية المستخدم في النفاذ إلى المعلومات بطريقة مريحة وآمنة (بدلاً من حمل حاسوب شخصي صغير مثلاً). من الممكنِ إعادةُ برمجة البطاقات الذكية أثناءَ استخدامها بحيثُ تُخَزَّنُ فيها رموزٌ مشفرةٌ جديدةٌ في كلِّ مرةٍ تُستعملُ فيها، وهذا يزيد فعلياً من صعوبة استعمالها بشكل غير نظامي.

يكمنُ السببُ وراء أهمية هذه البطاقات في أنها تزيد الخيارات التي تمتلكها الإدارة في ترقية النفاذ إلى النظام من كلمات السِّر فقط إلى مجموعة من التقنيات ومن رموزٍ تحددُ هوّية المستخدم. فالبطاقات الذكية رخيصةٌ نسبياً (حوالى 5 إلى 20 دولاراً)، وهي مريحة، وذات عمر طويل نسبياً. قد يستلزمُ الانتقالُ من نظام كلمة السِّر فقط إلى نظامٍ معززٍ بيولوجياً استثماراً قدره 250 دولاراً إلى 500 دولار لكلِّ محطة عمل. إن الترقيةَ إلى نظام البطاقة الذكية أرخصُ بكثيرٍ، ولكنه بالطَّبعِ لا يقدمُ المزايا التي تقدمها البيولوجيا.

فحص نظام أمن المعلومات

يشار إلى هذا الفحص غالباً بـ «اختبار الاختراق» أو «سَبْرُ الاستجابة». إن هذا الإجراء جزءٌ مهم من عملية التحقق من أن جميع الخطط والإجراءات التي يجب أن تكون جاهزة هي فعلاً جاهزة. يجرى فحص نظام أمن المعلومات هذا بعد تنفيذ تغييرٍ هامٍ في النظام المعلوماتي مثل تركيب البرمجيات أو ترقية نظام التشغيل. يُؤدَّى هذا الفحصُ غالباً من قبل جهةٍ استشاريةٍ مستقلةٍ أو منظمةِ أمنِ معلوماتٍ متخصصةٍ لتجنب التأثير الإداري أو السياسي غير الضروري. تجرى هذه الفحوصات في حالة أنظمة المعلومات التي تتطلب سرية عالية، وتجرى على أساس عشوائي ولكن مستمر للتثبت من استعمال آخر رُقَع البرمجيات، وإغلاق بوابات جدار النار غير اللازمة، وتقادم كلمة السِّر، وتفاصيلَ أخرى.

يجب على إدارة أمن تقنية المعلومات في المؤسسة أن تخطط للقيام بعمليات فحصٍ روتينية لضمان أن نشاطات النظام التشغيلية لم تَخْلِق فرصاً أو افتضاحات للنفاذ، فالقراصنة والمخترقون يبنون العديد من اعتداءاتهم على «افتراضات» يفترضها مديرو أمن المعلومات مثل: أن رقع البرمجيات قد نُصِبَتْ، وأن أجهزة المودم غير المستخدمة قد أزيلت، وأن كلمات سر الموظفين الذين تركوا المؤسسة قد حذفت.

تُصَنَّفُ نتائجُ الفحص في ثلاث فئات: «عالية» أو «متوسطة» أو «منخفضة» تبعاً لحساسية النتيجة. يستجاب إلى النتائج العالية وتُحَلُّ فوراً، أما النتائج المتوسطة فيستجاب إليها تبعاً للإمكانيات المتوفرة، وتُحلُّ النتائج المنخفضة كنشاط من أنشطة تطوير الحماية المستمرة.

يجبُ أن تُتابِعَ الإدارةُ العليا والمدراءُ التنفيذيونَ نتائجَ الفحصِ، وأن يلتمسوا التفاصيل حول ما تم القيام به للاستجابة إلى كل نتيجة من نتائج فحص أمن المعلومات. إن قيامَ المدراء بعقدِ اجتماعاتٍ شهريةٍ هي طريقةٌ يُحبَّذُ إتباعها لفهم ما يحدث (أو ما لا يحدث) ولماذا. ونظراً إلى وجود استثمار واضح لمالِ ولوقتِ الإدارة في عقدِ هذهِ الاجتماعات، يجب أن يصدرَ عنها استكمالُ أو تخطيطُ نشاطاتٍ مهمةٍ جداً لأمن المعلومات. ولكن نظراً إلى الطبيعة المستمرة للاعتداءات على أمن المعلومات، وللتطور المستمر في طرق الاستجابة لها وصدّها، سيكون غريباً عدم تناول عدة بنود «عملية»

لمناقشتها في هذه الاجتماعات على المستويين الإداري والتقني للمنظمة.

هيكل الممارسات الأفضل

الممارسة الأفضل (المثلى)	الحساسية	التكرار	المشاركون	نتائج النشاط
تحقق من أن كل الأنظمة قد زُوِّدَت بأحدث ترقيعات برمجيات أمن المعلومات وأنها تعمل.	عالية	عند الحاجة	أمن المعلومات، إدارة النظام	رقع برمجيات محدثة على جميع الأنظمة بأسرع وقت ممكن
تأكد من أن بنى أمن التطبيقات ونظام التشغيل على جميع الأنظمة العاملة لا تعدّل أو تُغيّر إلا من قبل مدراء النظام، وتحقق من ذلك	عالية	شهرياً	أمن المعلومات، مدراء النظام	إمكانية إدخال التغييرات مقصورة على المدراء فقط
تحقق من وجود سياسة التعامل مع البيانات المتقادمة وتأكد من أنها تُتَّبَع	عالية	فصلياً كل ثلاثة أشهر	الإدارة، أمن المعلومات	حفظ (أرشفة) البيانات المتقادمة مع إجراءات حماية كافية.
اختبر جميع أنظمة حفظ البيانات واستعادتها، وتأكد من أن الممارسات المتعلقة باسترجاع البيانات تعمل	عالية	شهرياً	أمن المعلومات، مدراء النظام	القدرة المؤكدة حفظ البيانات واستعادتها
تأكد من استلام جميع تراخيص البرمجيات وأن تكلفة الصحيح منها تدفع في وقتها.	متوسطة	فصلياً كل ثلاثة أشهر	الإدارة، المالية، مدراء النظام	الالتزام بشروط وبنود تراخيص البرمجيات
تحقق من أن عمليات التحكم بالنفاذ للنظام معقولة وأن تعريض أمن المعلومات للمخاطر قد تم تجنبه	متوسطة	فصلياً كل ثلاثة أشهر	الإدارة، المالية، مدراء النظام	الثقة في السماح بالنفاذ للشخص الصحيح وفقاً للسياسة
تأكد من أن نقاط النفاذ اللاسلكية تمتلك تعمية بمفتاح طوله 64 خانة على الأقل وأنها قد وُضِعَت بعيداً عن الأماكن غير الآمنة	عالية	عند تنصيبها، تُفحص فصلياً	أمن المعلومات، مدراء النظام	تعرض أقل للاعتداء اللاسلكي والنفاذ المحظور
عطل خيار بث «مُعَرِّف مجموعة الخدمة» «SSID» من نقاط النفاذ اللاسلكية	عالية	عند تنصيبها، تفحص فصلياً	أمن المعلومات، مدراء النظام	تَعَرُّضٌ أقل للاعتداء اللاسلكي وللنفاذ المحظور
حدد ما إذا كان اعتماد طريقة النفاذ بالبطاقة الذكية أو بالمؤثرات البيولوجية مناسباً تبعاً لقيمة المعلومات وعدد المستخدمين/ الزبائن الذي قد يتأثر.	متوسطة	فصلياً كل ثلاثة أشهر	الإدارة، المالية، مدراء النظام	حدد إذا كان ينبغي تحديث طرق أمن المعلومات بسبب تغيير أوضاع الشركة

الملخص

تستمرُ منتجاتُ تقنية أمنِ المعلوماتِ بالازديادِ من حيث التعقيدِ والأداءِ والمقدرةِ وذلك تلبيةً لمتطلبات السوق. لقد أصبح ما تقوم به هذه المنتجات، على مدار 24/ 7، أمراً مذهلاً، فهي تمنع النفاذ غير المرخص، وتراقب النشاطات الاقتحامية مع إيجاد الدليل لدعم الادعاء، وتنقل عدة جيغا بايت من البيانات بشكل شبه فوري. إلا أن هذه الأنظمة هي مجرد أجهزة الكترونية، فهي تتطلب صيانةً ودعماً هندسياً، كما أنها تتطلب التحديث باستمرار، وقبل كل شيء إنها بحاجة إلى إدارة موجهة.

إن الحرب العنيفة القائمة بين المجموعات والأشخاص الذين يحاولون النفاذ إلى أنظمة وأصول المعلومات التي لا ينبغي لهم الوصول إليها، والمنظمات التي تعمل بجد لإبقائهم بعيداً، هي معركة تكاد تكون مجهولة لدى المدراء التنفيذيين والإدارة العليا لانهماكهم بإدارة العديد من المسؤوليات الأخرى. تُبَلِّغُ الشركات الصغيرة في الولايات المتحدة عن 200 إلى 500 اصطدام بجدران نارها كلَّ ساعة من قبل محركاتِ بحثٍ اقتحاميةٍ غير محددةٍ تسعى إلى إيجاد ثغرات في جدار نارها للنفاذ من خلالها. من الصعب تصور وجود مئات الآلاف من عمليات البحث الاقتحامية كل يوم، والتي تتفاداها المنظمات الحكومية والمالية الضخمة بنجاح، ويعود ذلك إلى عدم الإعلان أو التنويه عن هذه العمليات في وسائل الإعلام العامة.

يبدو واضحاً أن الجمع بين التقنية، والنظرة المنطقية، والاهتمام بالتفاصيل، قد خطا خطوات متقدمة نحو سدِّ معظم الثغرات الكبرى في البنية التحتية لأمن المعلومات. إن الثغرات ستبقى ولكن جعل الثمرة أصغر من الجهد اللازم للحصول عليها يمنع القراصنة عادةً من إضاعة وقتهم في كسب القليل.

سيحتاج كبارُ المدراء والمدراءُ التنفيذيين في السنوات المقبلة إلى أن يصبحوا أكثرَ دراية بالمصطلحات والمفاهيم الأساسية لأمن المعلومات كي يدركوا بشكل أفضل دواعي دعمهم للاستثمارات المتزايدة في الأجهزة والموظفين. ووفقاً لخبراء في القانون وفي التقنية وفي الأعمال، سيبقى أمن الحاسوب جزءاً هاماً في عمل أي منظمة لعقود قادمة.

الفصل السابع

مواد ومواقع مرجعية

تصريح مكتب التحقيقات الفيدرالي الأمريكي حول تحسين أمن المعلومات

تصريح جيمس أي. فرنان، نائب مساعد المدير، في قسم شبكات الاتصال الالكتروني، لدى مكتب التحقيقات الفدرالي حول محاربة التلاعب وتحسين أمن المعلومات، وذلك بتاريخ 3 نيسان، 2003. قدّمَ هذا التصريح أمام لجنة الخدمات المالية التابعة للبيت الأبيض، واللجنة الفرعية حول المؤسسات المالية وائتمان المستهلك، وأمام لجنة المراقبة والتحقيقات، في واشنطن D.C.

(Farnan, 2003)

«أشكركم لدعوتي هنا اليوم لأفيد حول موضوع «محاربة التلاعب: تحسين أمن المعلومات». إن عقدَ هذه الجلسة، لسماع الشهادات، يثبت التزامكم بتحسين أمن أنظمة معلومات أمتنا ودعمَ هذه اللجنة للقضية في «الكونغرس». إن عملنا هنا مهمٌ جداً، لأن المخاطر المتضمنة جسيمةٌ. ستعالجُ شهادتي اليومَ نشاطاتِ قسم شبكات الاتصال الالكتروني في مكتب التحقيقات الأمريكي باعتبارها تتعلق بطيفٍ واسع من الأعمال الإجرامية المتعلقة بالغش وأمن المعلومات. يوجد اليوم أكثر من 180 مليون مستخدم للحاسوب في الولايات المتحدة وحدها، كما يوجد أكثر من 600 مليون في أنحاء العالم، والعدد في ازدياد. إن العديد من هؤلاء المستخدمين يتصلون بالإنترنت، ويتواصلون مع

بعضهم البعض، ويديرون عملاً، ويشرفون على شؤون مالية، ويبحثون عن المعلومات، ولسوء الحظ يرتكبون الجرائم.

ثغرات شبكات الاتصال الالكتروني

إنَّ أيَّ شخصٍ يبدي اهتماماً أساسياً بالحاسوب سيكون مُدركاً لوجود ثغرات أمن المعلومات، على الأقل بمعناها العام، في شبكاتنا وحواسبينا. تُناقَشُ هذه الثغرات بشكلٍ واسعٍ في وسائل الإعلام، وباستخدام بسيط للبحث على الإنترنت، يستطيع طفلٌ بِعمرِ 12 عاماً اكتشافَ أدواتِ قرصنةٍ مختلفة، ومن ثم تحميلها واستعمالها. عندما رأينا في البداية الازديادَ المفاجئَ في الحواسيب المنزلية في أوائل 1990م، لم نقلق بشأن الاعتداءات على حواسب أسرنا. لم يكن أغلب المستخدمين غير الرسميين مدركين حتى لوجود الثغرات الأمنية. إننا نقلقُ اليومَ من إصابة أنظمتنا بالفيروسات، والديدان وأحصنة طروادة. تقوم الشركات بحماية المواقع والصفحات الالكترونية من الاعتداءات وعمليات التشويه. إن المستهلكين قلقون أن لا تكون الشركات محافظةً على حمايةٍ كافيةٍ لمعلوماتنا المالية والشخصية، إذ نسمع تقارير إخبارية أسبوعية حول القراصنة واقتحامات جديدة.

تعتمد الشركاتُ والمستهلكون الأمريكيون بشكل متزايد على الإنترنت لعقد صفقاتهم، فالتجارة الالكترونية تنمو في جميع قطاعات اقتصاد الولايات المتحدة. إن أغلب صفقات التجارة الالكترونية هي من شركة إلى شركة، ولكن مبيعات التجزئة للتجارة الالكترونية وصلت إلى 46 بليون دولار في عام 2002م، وأكثر من 36 بليون دولار في عام 2001م. عندما يتوقف عمل مستخدمي الإنترنت ـ سواء أكانوا شركات أو مستهلكين ـ بسبب أعمال الغش أو التزوير على الإنترنت، فإن نجاح التجارة الالكترونية مهدد بالإخفاق.

إن اختراقات الحاسوب فئة مختلفة عن أغلب أعمال الغش أو التزويد، فالعديد من الانتهاكات لا يتم الإبلاغ عنها، لأن الشركات تخشى خسارةَ التجارةِ بسبب فقدانِ ثقة المستهلكِ في إجراءات أمنِ المعلوماتِ لديها، أو بسببِ الخوفِ من الادعاءات القضائية. إن أغلبَ قضايا انتهاكات أمن المعلومات المنشورة اليوم هي نتيجة لفشل ترقيع الثغرات المعروفة التي من أجلها أُصدرت الرقع. قد تتيسر سرقة معلومات المستهلك من نظام الحاسوب بطريقتين:

بوساطة المطلعين العاملين من داخل المؤسسة أو من قبل القراصنة الغرباء. يمتلك المطلعون دوافع مختلفة، بما في ذلك المكسب أو المال، أما الغرباء فيدفعهم عادة التحدي و/أو الطمع.

أصدر مجلس البحث الوطني بياناً في عام 2001م بعنوان «أمن شبكات الاتصال الالكتروني اليوم وغداً: ادفع الآن أو ادفع لاحقاً». إذا لم تطلعوا على هذا البيان فإني أحثكم على اقتناء نسخةٍ منه. يصوغ البيان مجموعة من النقاط الهامة، والملاحظات العامة، بما في ذلك نقطة جوهرية من أجل هذه الجلسة:

«لاحظ أيضاً أن المعتدي. . . قد يكون قادراً على استغلال خطأ أُحْدِثَ مصادفةً في النظام، فتصميمُ النظام و/أو التطبيقُ الرديء قد يؤدي إلى مشاكل أمنِ معلوماتٍ خطيرة، ربما تكون هدفاً أو ربما تستهدف عمداً في محاولة اختراق من قبل المعتدي».

إذا كانت حمايةُ النظام غيرَ كافيةٍ، واختار شخص ما استغلال نقاط الضعف، فإن العواقب ستكون حتمية. ووفقاً لهذا البيان توجد ثلاثة أشياء قد تحبط نظام الحاسوب أو الشبكة:

1. **قد يصبح غير جاهز أو بطيئاً جداً،** أي أن استخدام النظام أو الشبكة يصبح مستحيلاً أو قريباً من ذلك.

2. **قد يصبح محرفاً** ويقوم بالشيء الخاطئ أو يعطي إجابات خاطئة. على سبيل المثال: قد تصبح البيانات المخزنة على الحاسوب مختلفة عمّا يجب أن تكون، وهذا مشابه لحالة تعديل السجلات المالية أو الطبية الورقية بشكل غير ملائم.

3. **قد يصبح راشحاً.** أي أن الشخص الذي لا ينبغي له الوصول إلى بعض أو جميع المعلومات المتوفرة على الشبكة يصبح قادراً على ذلك.

عندما تحدث واحدة من هذه الأشياء، فإن مكتب التحقيقات الفدرالي هو الجهة المعنية بالاستجابة، لأنها الوكالة الفيدرالية الوحيدة التي تمتلك السلطة القانونية، والخبرة والقدرة على الجمع بين محاربة الإرهاب، والاستخبارات المضادة، والموارد اللازمة لإبطال الأعمال الإجرامية، والحد من العمليات غير القانونية التي تستهدف الحاسوب.

قسم شبكات الاتصال الالكتروني في مكتب التحقيقات الفدرالي (FBI)

تتضمن إعادة تنظيم مكتب التحقيقات الفدرالي للسنتين الأخيرتين هدفَ جعلِ الموارد الاستخباراتية لشبكات اتصالنا الالكتروني أكثر فعالية. في عام 2002م أدَّت إعادة التنظيم إلى تأسيس قسم شبكات الاتصال الالكتروني في المكتب.

يعالج قسمُ شبكات الاتصال الالكتروني تهديدات شبكات هذا الاتصال معالجةً منسقةً سامحاً للمكتب بالبقاء، من النواحي التقنية، متقدماً خطوة على خصوم شبكات الاتصال الالكتروني ومهدديها. يتعامل قسم شبكات الاتصال الالكتروني مع جميع انتهاكات الاتصال الالكتروني التي لها غالباً تبعات عالمية وانعكاسات اقتصادية وطنية. يدعم هذا القسم أيضاً أولويات المكتب في إطار برنامجه في محاربة الارهاب، والاستخبارات المضادة، والتحقيقات الإجرامية الأخرى عندما تكون الإعانة الاستخبارية التقنية مطلوبة. يتعهد القسم بأن يتوفر لديه خبراءٌ ذوو مهارات تقنية متخصصة يركزون على القضايا المرتبطة بشبكات الاتصال الالكتروني.

إننا نتناول في قسم شبكات الاتصال الالكتروني منهجيةً مؤلفةً من اتجاهين للمشكلة. يتعامل الاتجاه الأول مع النشاط الإجرامي التقليدي الذي انتقل إلى الإنترنت، مثل الغش أو التزوير على الإنترنت، وسرقة الهوية على الخط، والكتابات أو الصور الإباحية عن الأطفال على الإنترنت، وسرقة أسرار التجارة، والجرائم المشابهة أخرى. يتعامل الاتجاه الآخر غير التقليدي مع الأنشطة الجديدة التي أتاحتها الإنترنت و لم تكن موجودةً قبل تأسيس الحواسيب والشبكات والإنترنت. يشمل هذا الاتجاه إرهاب «شبكات الاتصال الالكتروني»، والتهديدات الإرهابية، وعمليات الاستخبارات الخارجية والنشاط الإجرامي المتمثل بانتهاكات الحاسوب غير القانونية داخل شبكات حاسوب الولايات المتحدة بما في ذلك تعطيل العمليات الداعمة للحاسوب وسرقة البيانات الحساسة بواسطة الإنترنت. يتوقع المكتب انتشار تهديد شبكات الاتصال الالكتروني بسرعة، نظراً إلى أن عدد الفاعلين القادرين على استخدام الحواسيب لأغراض غير قانونية مضرة ومدمرة هو في ازدياد.

لإتمام مهمته، سيشكل قسم شبكات الاتصال الالكتروني تحالفات بين القطاعين العام والخاص معززة بالتدريب والتعليم ليزيد من قدرات الاستجابة لمهددات شبكات الاتصال الالكتروني أي: محاربة الإرهاب، والاستخبارات المضادة، وتطبيق القانون. سيزيد المكتب كذلك من نجاح تحقيقات شبكات الاتصال الالكتروني من خلال زيادة الوعي واستغلال التقنية الجديدة.

إننا نضاعف جهودنا الاستخباراتية العالمية وبرامج تدريبنا على شبكات الاتصال الالكتروني لدعم هذه المهمة. وبالنتيجة فقد تم الآن خلق وحدات مخصصة في المركز الرئيسي للمكتب لتقدم تدريباً ليس فقط لفرق شبكات الاتصال الالكتروني للمكتب وحسب، وإنما أيضاً للوكالات الأخرى المشاركة في الحملات الجديدة أو المرتبطة بهذه الشبكات التي يكون المكتب عضواً مشاركاً فيها. سيُعطَى هذا التدريب غالباً إلى المحققين في المجال وستُدَرَّسُ مجموعةٌ من المواد في أكاديمية المكتب في كوانتيكو.

تُرفع القضايا إلى المكتب من خلال مركز الادعاء ضد التلاعب عبر الإنترنت Internet Fraud Complaint Center (IFCC)، الذي أَثْبَتَ في عامه الرابع من العمل على أنه دار مقاصة ناجحة، متلقياً أكثر من 75,000 شكوى في عام 2002م بشأن جرائم تتراوح من سرقة الهوية وانتهاكات الحاسوب إلى إباحية ضد الأطفال.

إذا تلقى مركز (IFCC) تقريراً بشأن اقتحام ما من شركة في بيرمينغهام ـ ألباما مثلاً فإننا سنحاول أولاً تعيين مكان حدوث الانتهاك. قد تكون الخدمات الحاسوبية لهذه الشركة في منيبوليس، بينما يوجه المعتدي الهجمات من خلال مزودي الإنترنت في كاليفورنيا وأوروبا. إذا جرت قرصنة المخدِّمات في مينيبوليس، فإن فريق عمل المركز في منيبوليس لجريمة شبكات الاتصال الالكتروني سيكلَّفُ بقيادة القضية. قد تبدأ خيوط القضية في كاليفورنيا، ولكنها تنتهي في أوروبا الشرقية، أو نيجيريا، أو تعود إلى بيرمينغهام إذا كان أحد المعنيين موظفاً من داخل الشركة. سيُطْلَبُ فريقٌ من فِرَقِ الاستجابة للتحليل الحاسوبي التابع للمكتب Computer Analysis Response Team (CART) لإيجاد الأدلة القضائية للحاسوب، وقد يُرْسَلُ هذا الدليلُ إلى واحدٍ من مختبراتنا الإقليمية الجديدة القائمة الآن في شيكاغو أو دالاس أو سان دييغو. سيحدد

المختبر مدى الانتهاك ومدته، وما إذا كان المعتدي ينطلق من داخل أو خارج الشركة. قد تُحلُّ المسألةُ في بضعة أيامٍ، أو قد تأخذ عدة سنوات تبعاً لحنكة المعتدي. تكون القضايا معقدةً بشكل دوري وتتضمن غالباً اتصالات عالمية.

تفيدُ القضايا التالية كأمثلة على الجرائم النموذجية لشبكة الاتصال الالكتروني:

ريموند توريسيلي، المعروف بـ «روليكس»:

إن ريموند توريسيلي، المعروف بـ «روليكس»، قائد فريق القراصنة المعروف بـ «Conflict#»، قد أدين بسبب اقتحام حاسوبين، بين أشياء أخرى، مقتنين ومصانين من قبل «مختبر الدفع النفاث» التابع للهيئة الوطنية لإدارة أبحاث الملاحة الجوية والفضاء الموجود في باسدينا، كاليفورنيا، واستخدام واحدٍ من هذين الحاسوبين ليضيف غرفة محادثةٍ إلى الإنترنت مكرَّسةٍ للقرصنة.

لقد اعترف توريسيلي أنه كان في 1998م قرصانَ حاسوبٍ، وعضواً في منظمة القرصنة المعروفة بـ «Conflict #». أقر توريسيلي بأنه كان يستخدم حاسوبه الشخصي لتشغيل برامج مصممة للبحث في الإنترنت وللتحري عن الحواسيب القابلة للاعتداء. حالما يتم تعيين أمكنة مثل هذه الحواسيب، يحصل حاسوب توريسيلي على النفاذ غير القانوني إلى الحواسيب بواسطة تحميل برنامج معروف بـ «رووت كيت» Rootkit. إن ملف «رووت كيت» هو برنامج يسمح للقرصان عندما يشغل الحاسوب بإحراز النفاذ الكامل إلى جميع وظائف الحاسوب بدون أن يقوم المستخدمون المخولون لذلك الحاسوب بمنح هذه الامتيازات.

استُخدِمَ أحد الحواسيب الذي دخله توريسيلي من قبل الوكالة الوطنية لإدارة أبحاث الملاحة الجوية والفضاء (NASA) لإنجاز تصميم القمر الصناعي وتحليل المهمة الخاصة بمرحلات الفضاء المقبلة، استُخدِمَ الحاسوب الآخر من قبل قسم الأنظمة الأرضية للاتصالات كمخدِّمِ الشبكة الداخلية والبريد الالكتروني التابع لمختبر الدفع النفاث. بعد إحرازَ الدخول المحظور إلى الحواسيب وتحميل «رووت كيت»، استعمل توريسلي اسمه

المستعار «روليكس» في العديد من الحواسيب ليضيف مناقشات غرفة المحادثة (chatting).

اعترف توريسيلي أنه دعا في هذه المناقشات المشاركين بالمحادثة إلى أن يقوموا بزيارة موقع إلكتروني يعرض فيه صوراً إباحية، وأنه كسب 18 سينتاً عن كلِّ زيارة يقوم بها الشخص لذلك الموقع. لقد حصل توريسيلي تقريباً على 300 ـ 400 دولار أسبوعياً من هذا النشاط. اعترف توريسيلي كذلك بجريمة اعتراض كلمات السِّر وأسماء المستخدمين المتداولة على الشبكات الموصولة بالحاسوب المقتنى من قبل جامعة ولاية سان جوس. بالإضافة إلى ذلك، اعترف بجريمة الاستيلاء على كلمات سِّر وأسماء مستخدمين مسروقة استخدمها للحصول على نفاذٍ مجاني للإنترنت أو لإحراز دخولٍ محظور إلى حواسيب أكثر.

أقر توريسيلي أنه عندما كان يحصل على كلمات سر معماة (مشفرة)، فإنه يستخدم برنامج فك تعمية (كسر) كلمة السِّر المعروف بـ «جون الممزِق» John The Ripper لفك تشفير كلمات السِّر، كما صرح بجريمة امتلاك أرقام بطاقات ائتمان مسروقة حصل عليها من أشخاص آخرين وخزنها على حاسوبه. اعترف توريسيلي أنه استخدم مثل هذا الرقم الخاص ببطاقة الائتمان لشراء خدمة اتصالات هاتفية بعيدة المدى.

إن المزيد من الدلائل التي حُصِل عليها ضد توريسيلي قد تم التوصل إليها من خلال تفتيش حاسوبه الشخصي، فإلى جانب الآلاف من كلمات السِّر المسروقة والأرقام الهائلة لبطاقات الائتمان، وَجَدَ المحققون نسخاً من مناقشات غرفة المحادثة التي قد تباحث فيها كل من توريسيلي وأعضاء «Conflict #» وسط أشياء أخرى مثل:

1. اقتحام حواسيب أخرى.

2. الحصول على أرقام بطاقات ائتمان تعود إلى أشخاص آخرين واستخدام هذه الأرقام للقيام بصفقات محرمة.

3. استعمال حواسيبهم ليغيروا الكترونياً نتائج جوائز أفلام (MTV) السنوية. تبين هذه القضية التنوع الكبير للأعمال الإجرامية التي قد تنشأ عن ثغرات أمن المعلومات.

رافال غري، المعروف بـ «كوريدور»:

في 1 آذار/مارس عام 2000م كَشَفَ قرصانُ الحاسوب، الذي انتحلَ اسم «كوريدور»، مواقعَ إلكترونية عديدة للتجارة الإلكترونية في الولايات المتحدة، وكندا، وتايلند، واليابان، والمملكة المتحدة وسَرَقَ حوالى ثمانية وعشرين ألف رقم لبطاقات ائتمان، مع خسائر مقدرة على الأقل بـ 3.5 مليون دولار. لقد وُضِعَتْ الآلافُ من أرقام بطاقات الائتمان وتواريخ انتهاء كل منها على مواقع الكترونية عديدة. قام مكتب التحقيقات الفدرالي بإجراء تحقيقات موسعة في 23 آذار/مارس عام 2000م، بالتعاون مع ديفيد بويز (المملكة المتحدة ـ ويلز)، والشرطة، وفي التفتيش في منزل «كوريدور»، رافال غري. اعتُقل السيد غري البالغ من العمر 18عاماً واتُهم في المملكة المتحدة، مع شريكٍ له في التآمر، بمقتضى قانون سوء استخدام الحاسوب بالمملكة المتحدة لعام 1990م. تبين هذه القضية فوائد تطبيق القانون والتعاون مع الصناعة حول العالم بشأن تحقيقات جريمة الحاسوب.

ابتزاز «بلو بيرغ»:

اعتقل المواطنان الكازاخستانيان أوليغ زيزوف وزميله ايغور ياريماكا في 10 آب/أغسطس 2000م في لندن، إنكلترا، نظراً إلى اقتحامهما نظام حاسوب مانهاتان لشركة بلومبيرغ (Bloomberg L.P.) في محاولة لابتزاز المال من السيد بلومبيرغ. تمكن زيزوف من النفاذ المحظور إلى نظام حاسوب بلومبيرغ الداخلي من حواسيب موضوعة في ألماتا ـ كازاخستان. في ربيع عام 1999م كانت شركة بلومبيرغ تقدم خدمات قاعدة بيانات من خلال النظام المعروف بـ «بلومبيرغ المفتوح» إلى مؤسسة كازكومريرتس المالية القائمة في ألماتي، كازاخستان، وكان زيزوف موظفاً من كازكومرتس.

أرسل زيزوف مجموعةً من الرسائل الالكترونية إلى ميشال بلومبيرغ منشئِ ومالكِ بلومبيرغ مستخدماً اسم «اليكس» مطالباً أن يدفع له بلومبيرغ مبلغ 200.000 دولار، مقابل قيامه بتزويد بلومبيرغ بمعلومات بخصوص كيفية تمكن زيزوف من التسلل إلى نظام حاسوب بلومبيرغ. أرسل ميشال بلومبيرغ بريداً الكترونياً إلى زيزوف مقترحاً أن يلتقوا مع بعضهم بعضاً. طالب زيزوف ميشال بلومبيرغ أن يودع 200.000 دولار في حسابٍ له خارج كازاخستان. أنشأ بلومبيرغ

حساباً في البنك الألماني في لندن وأودع 200.000 دولار. اقترح ميشال بلومبيرغ أن يقوموا بحل المشكلة في لندن ووافق زيزوف.

في 6 آب/أغسطس عام 2000م ذهب كل من زيزوف وزميله ياريماكا من كازاخستان إلى لندن. في 10 آب/أغسطس عام 2000م، التقى ياريماكا وزيزوف مع موظفين من بلومبيرغ (L.P) ومعهم ميشال بلومبيرغ، وشرطيين من العاصمة لندن، تظاهر الأول على أنه موظفٌ إداري كبير في بلومبيرغ (L.P) والثاني على أنه مترجم. ادعى ياريماكا في المقابلة أنه كان نائباً عاماً سابقاً لـ كازاخستان، وبيّن أنه يمثل «اليكس» وسوف يدير شروط الدفع. ووفقاً للادعاء كرر كل من ياريماكا وزيزوف مطالبهما في المقابلة. اعتقل كل منهما بُعَيد الاجتماع. في 27 شباط/فبراير 2003م انتهت محاكمة انا تولجيفيش زيزوف بالحكم الإجرامي بسبب التلاعب بالحاسوب، والابتزاز، واستخدام الاتصالات المتعلقة بأكثر من ولاية من أجل الابتزاز والتآمر. إنه يواجه 28 عاماً في السجن. هذه القضية هي مثال للجريمة التقليدية التي سهّلها الحاسوب.

تستمر جرائم شبكات الاتصال الالكتروني بالازدياد بمعدل يثير المخاوف، وتساهم الثغرات في المشكلة. إننا نشجع المدراء ومحترفي أمن المعلومات على تقليل الفرص للمجرمين من خلال توظيف الممارسات الأفضل وترقيع الثغرات قبل أن يتم استغلالها. سيواصل مكتب التحقيقات الفيدرالي ملاحقة مجرمي شبكات الاتصال الالكتروني باعتبارنا نكافح للبقاء متقدمين عليهم خطوة في سباق تقنية جريمة شبكات هذا الاتصال.

أشكركم على دعوتكم لي لأحدثكم اليوم، وبالنيابة عن المكتب أتطلع بأمل ولهفة إلى العمل معكم في هذا الموضوع بالغ الأهمية.

إحصائيات حول جرائم الحاسوب

إن المصدر المرجعي الممتاز لإحصائيات جرائم الحاسوب هو الموقع الالكتروني لمعهد أمن الحاسوب Computer Security Institute (CSI) (www.gocsi.com). هناك رابط، في موقع المعهد على الإنترنت، يحتوي على تقرير المعهد الخاص بالمسح السنوي لجرائم الحاسوب. يُجري المعهدُ هذا المسح بالتعاون مع المركز الوطني لحماية البنية التحتية (NICP) التابع لمكتب التحقيقات الفدرالية. إن (NICP) هو عبارة عن تعاون بين الصناعة ووكالات

فيدرالية عديدة، وهو مهيّأ ليكون منظمة أساسية من أجل التعامل مع الجرائم المنفذة باستخدام الحاسوب والاعتداءات المستهدفة لبنية الأمة التحتية التشغيلية، بما في ذلك المطارات، والطرق العامة، وشبكات المواصلات السلكية واللاسلكية والأبنية الحكومية.

يقدم التقريرُ السنوي عن المسح، والقابل للتحميل مجاناً من موقع (CSI) على الإنترنت، معلومات واضحة ـ مع نتائج أخرى ـ حول أنواع جرائم الحاسوب المقترفة، والمصادر الممكنة، ومتى تم الإبلاغ عنها وإلى من، وقيمة الخسائر. يجرى المسح كل سنة وينشر في أواخر آذار/مارس، بداية نيسان/أبريل. وغالباً ما يصبح التقرير عند نشره مصدراً إعلامياً للتنبُؤِ باتجاهات جريمة الحاسوب، وتقنيات الردع، ولقياس الزيادة في ظهور الجريمة من سنة إلى سنة، وتوقعات الخسائر المالية إذا ما فشلت إجراءات الحماية المضادة.

مصادر مرجعية حول جدار النار

يوجد العديد من الكتب التي تقدم معارف عامة ممتازة حول جدران النار. منها ما يلي:

- Cheswick, B. and Bellovin, S. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker*. ISBN 0-201-63357-4. Addison Wesley.
- Garfinkel, S., and Spafford, G. (1996). *Practical Internet and Unix Security*. ISBN 1-56592-148-8. O'Reilly Books.
- Zwicky, E. D., Cooper, S., and Chapman, D. B. (2000). *Building Internet Firwalls*. 2nd ed. ISBN 1-56592-871-7. O'Reilly Books.

من المراجع الإضافية ذات العلاقة ما يلي:

- Comer, D. and Stevens, D. (1992). *Inernetworking with TCP/IP* (vols. I, II, III). ISBN 0-13-468505-9(I), 0-13-472242-6(II), 0-13- 474222-2(III). Prentice-Hall.

(مناقشة مفصلة حول هندسة الإنترنت وتطبيقها وبروتوكولاتها. إن المجلد الأول الذي يتحدث عن المبادئ، والبروتوكولات والهندسة قراءته ممكنة من قبل كل شخص، أما المجلد الثاني فهو (حول التصميم، التطبيق والأمور

الداخلية) ميال إلى التقنية بقدر أكبر. ويغطي المجلد الثالث خادم الزبائن المرتبط بالحاسوب)

- Curry, D. (1992). *Unix System Security - A Guide for Users and System Adminstrators*. ISBN 0-201-56327-4. Addison Wesley.

معلومات من الإنترنت حول جدران النار

قائمة بريد جدران النار (http://lists.gnac.net/firewalls) (Curtin, 2000)

إن قائمة بريد جدران النار للإنترنت هي عبارة عن منتدى من أجل مدراء ومنفذي جدار النار. للاشتراك أرسل «اشترك في جدران النار» في الرسالة (وليس في سطر موضوع الرسالة) إلى (majordomo@lists.gnac.net).

معلومات حول «الكيفية» لبناء جدار النار

- يصف هذا الموقع ما هو مطلوب من أجل بناء جدار النار، وخاصة مع استخدام الينوكس.

http://sunsite.unc.edu/LDP/HOWTO/firewall-HOWTO.html.

- مجموعة أدوات جدار النار (FWTK) وأوراق جدار النار: (ftp://ftp.tis. com/pub/firwalls).
- المنشورات المتعلقة بجدار النار لماركوس رانوم (http://www.ranum. com/pubs).

أبحاث حول جدران النار والاقتحامات

- (ftp://ftp.research.att.com/dist/internet_security)
- أدوات حماية جامعة (Texas A&M): (http://www.net.tamu.edu/ftp/ security/TAMU)
- صفحة جدران النار للإنترنت مشروع COAST: (http://www.cs. purdue.edu/coast/firewalls).

الثبت التعريفي

[مجموعة من هذه المصطلحات مقتبسة من شركة (Set Solutions Inc. 2004)]

سوء استعمال الامتياز Abuse of Privilege: عندما يقوم المستخدمون بعملٍ لا يتوجب عليهم القيام به وفقاً لقانون أو سياسة تنظيمية.

قوائم التحكم بالنفاذ Access Control Lists: هي قواعد تخزن في المرشحات (مثل أجهزة الموجهات (routers تقوم بتحديد كتل المعلومات التي يسمح لها بالدخول وتلك التي ينبغي أن تحظر.

مُوَجِّه النفاذ Access Router: هو الموجِّه الذي يربط شبكتك بالإنترنت الخارجية.

جدار النار لطبقة التطبيقات Application-Layer Firewall: هو نظام جدار النار الذي يقدم الخدمة من خلال العمليات التي تحافظ على الاستمرارية وعلى وضعية كاملة لاتصال بروتوكول التحكم بالنقل (TCP). تعيد جدران النار لطبقات التطبيقات عنونة حركة سير المعلومات بحيث تظهر حركة السير الصادرة على أنها تولدت من جدار النار بدلاً من المضيف الداخلي.

التحقق من الهوية Authentication: هو عملية تحديد هوية المستخدم الذي يحاول النفاذ إلى النظام.

أمارة التحقق من الهوية Authentication Token: هي وسيلة قابلة للحمل مستخدمة من أجل التحقق من هوية المستخدم. تعمل هذه الأمارات بوساطة التحدي/ الاستجابة أو سلسلة رموز قائمة على الوقت أو بوساطة تقنيات أخرى. قد يتضمن هذا قوائم على الورق لكلمات سر سابقة.

السماح أو التخويل Authorization: هي عمليات تحديد أنواع النشاطات المسموح بها. يجري السماح عادة في سياق عملية التحقق من الهوية، ففور التحقق من هوية المستخدم، يُسمحُ له بأنواع محددة من الدخول أو النشاط.

المضيف المحصَّن Bastion Host: هو نظام قد تمّت تقويته ليقاوم الاعتداء، ويركب على الشبكات التي يتوقع خضوعها للاقتحام. إن المضيفات المحصنة هي غالباً أجزاء من جدران النار أو قد تكون خارج مخدمات الشبكة أو أنظمة الدخول للعامة. يعمل المضيف المحصن عادةً تحت نظام للتشغيل متعدد الاستعمالات (على سبيل المثال، اليونيكس، NT، VMS، ...الخ) بدلاً من نظام تشغيل البرمجيات المخزنة بطريقة لا يمكن تغيرها (Filmware) أو من النظام القائم على ذاكرة القراءة فقط.

التحدي/ الاستجابة Challenge/Response: هي تقنية للتحقق من الهوية يرسل بواسطتها المخدِّم تحدياً لا يمكن التنبؤ به إلى المستخدم الذي يحسب الاستجابة مستخدماً نوعاً من أمارة التحقق من الهوية.

الجمع الفاحص التعموي (التشفيري) Cryptographic Checksum: هو تابع حسابي وحيد الاتجاه يطبق على الملف لحساب «بصمة» خاصة بالملف من أجل مراجعة لاحقة. إن أنظمة الجمع الفاحص هي وسائل أساسية لكشف ملفات النظام الخبيثة على اليونيكس.

الاعتداء المسيَّر بالبيانات Data Driven Attack: هو شكل من أشكال الاعتداء يتم فيه ترميز الاقتحام برموز تبدو بريئة ضمن البيانات وهو يُنفذ من قبل المستخدم أو برمجيات أخرى لتحقيق الانتهاك. في حالة الجدران النارية يكون الاختراق المسير بالبيانات مصدراً للقلق باعتباره قد يخترق الجدار الناري على شكل بيانات، ويشن هجوماً ضد النظام خلف الجدار الناري.

الدفاع في العمق Defense in Depth: هو منهج من مناهج أمن المعلومات تجري منه حماية كل نظام على الشبكة إلى أقصى درجة. قد يستخدم بالارتباط مع الجدران النارية.

خداع نظام اسم النطاق DNS Spoofing (DNS): هو انتحال اسم (DNS) يخص نطاقاً لنظام آخر، إما بوساطة تغيير ذاكرة خدمة حفظ الأسماء التابعة للنظام الضحية أو بوساطة انتحال شخصية مخدِّم اسم النطاق من قبل مخدِّم آخر.

الموجِّه المُعمِّي (المُشفِّر) Encrypting Router: انظر في تعريف الموجه عبر الأنفاق Tunneling Router، أو الحدود الخارجية للشبكة الافتراضية Virtual Network Perimeter.

جدار النار Firewall: هو نظام أو مجموعة من الأنظمة تقوي حدود الحماية بين شبكتين أو أكثر.

أمن المعلومات القائم على المضيف Host-based Security: هي تقنية لحماية نظام ما من الاعتداء. إن الحماية القائمة على المضيف هي نظام التشغيل وتعتمد على النسخة التي تستعملها منه.

اعتداء من الداخل Insider Attack: هو الاعتداء المولّد من داخل الشبكة المحمية.

كشف الاختراق Intrusion Detection: هو الكشف عن الاقتحامات أو محاولات الاقتحام إما يدوياً أو بوساطة برمجيات نظم خبيرة تعمل على سجلات الأداء (Logs) أو على معلومات أخرى متوفرة على الشبكة.

سرقة/ اختطاف (IP) IP Splicing/Hijacking: هو الاعتداء الذي يتم فيه تعطيل أو اقتحام جلسة تواصل قائمة عبر الإنترنت من قبل مُعتَدٍ. قد تحدث اعتداءات اختطاف (IP) بعد أن يتم إجراء التحقق من الشخصية سامحاً للمقتحم أن ينتحل وظيفة المستخدم المباح للتو. تعتمد الإجراءات الأساسية للحماية من اختطاف (IP) على التعمية في طبقة الجلسة أو طبقة الشبكة، من طبقات الاتصال السبع المعروفة.

خداع الـ (IP) IP Spoofing: هو الاعتداء الذي يحاول فيه النظام المعتدي انتحال صفة نظام آخر بشكل غير شرعي من خلال استخدام عنوان شبكة الـ (IP) خاصته.

الامتياز الأدنى Least Privilege: هو تصميم خصائص النظام التشغيلية للعمل بالقدر الأدنى من امتياز النظام. يقلل هذا من مستوى سماح تنفيذ العديد من الأفعال، ويخفف من الفرصة التي قد تسببها العملية أو المستخدم ذو الامتيازات العالية للقيام بنشاط محظور مؤدياً إلى خلل في أمن المعلومات.

تدوين الأحداث Logging: هو عملية تخزين المعلومات المتعلقة بالأحداث التي تقع على جدار النار أو الشبكة.

معالجة سجل (أو مدوّنة) الأحداث Log Processing: كيف تتم معالجة سجلات الرقابة وتفحصها من أجل الأحداث الجوهرية أو تلخيصها.

فترة حفظ سجل (مدونة) الأحداث Log Retention: ما هي المدة التي يتم فيها حفظ سجلات الرقابة وصيانتها.

جدار النار لطبقة الشبكة Network-Layer Firewall: هو الجدار الناري حيث تُفحص حركة السير في طبقة كتلة معلومات بروتوكول الشبكة.

الحماية القائمة على محيط الشبكة Perimeter-based Security: هي تقنية لحماية الشبكة بوساطة التحكم بالنفاذ إلى جميع نقاط الشبكة المخصصة للدخول والخروج.

السياسة Policy: هي القواعد الموضوعة على مستوى المنظمة والتي تضبط الاستخدام المناسب للموارد المتعلقة بالحواسيب، وممارسات الحماية، والإجراءات التشغيلية.

المخدِّم الوكيل Proxy: هو وكيل برمجي يعمل لمصلحة المستخدم. عادةً، يقبل الوكلاء الاتصال من المستخدم ويتخذون القرار بخصوص ما إذا كان عنوان بروتوكول الإنترنت (IP) للزبون أو المستخدم مسموحاً أو ممنوعاً من استخدام الوكيل، كما يمكن أن يقوم بإجراء تحقيقات إضافية بعد ذلك يكمل الاتصال لمصلحة المستخدم إلى الموقع المطلوب.

سرقة الجلسة Session Stealing: (راجع أيضاً تعريف سرقة/اختطاف (IP)، والهندسة الاجتماعية) هو اعتداء مرتكز على خداع المستخدمين أو المدراء في الموقع المستهدف. تنفذ اعتداءات الهندسة الاجتماعية عادةً بوساطة الاتصال بالمستخدمين أو العاملين والتظاهر بأنها مستخدم مباح لمحاولة إحراز النفاذ غير الشرعي إلى الأنظمة.

علم إخفاء البيانات داخل الصور أو الصوت Steganography: يرتكز إخفاء البيانات داخل الصور أو الصوت حاسوبياً على مبدأين. الأول هو أن الملفات التي تحتوي على صور أو أصوات محولة إلى إشارة رقمية قد تُغيَّر بدون فقد وظيفتها، على خلاف الأنواع الأخرى من البيانات التي يجب أن تكون دقيقة لتعمل كما يجب. يتناول المبدأ الثاني عدم قدرة الإنسان على تمييز التغيرات الثانوية في لون الصورة أو جودة الصوت.

حصان طروادة Trojan Horse: هو كيان برمجي يظهر وكأنه يقوم بأمر طبيعي ولكنه في الحقيقة يحتوي على برنامج للاعتداء أو على باب المصيدة.

مُوَجِّه عبر الأنفاق Tunneling Router: هو مُوَجِّهٌ أو نظامٌ قادرٌ على توجيه حركة سير المعلومات بعد تعميتها (تشفيرها) ووضعها في كبسولة رقمية وإرسالها عبر شبكة غير موثوقة، ليجري فك الكبسولة المعماة من قبل المستلم.

محيط الشبكة الافتراضية Virtual Network Perimeter: هي شبكة تظهر على أنها شبكة منفصلة محمية خلف جدران النار، وهي في الحقيقة تشتمل على قنوات اتصال افتراضية معماة عبر شبكات غير موثوقة.

الفيروس Virus: هو سلسلة من الرموز ترفقُ نَفْسَها على ملف للبيانات أو على برنامج ما، وتكرر ذلك بشكل واسع. قد تحتوي الفيروسات أو لا تحتوي على برامج للاعتداء، أو على أبواب المصيدة.

الدودة Worm: هي برنامج مستقل ينسخ نفسه من مضيف إلى آخر، ويُشغِّلُ نفسه بعد ذلك على كل مضيف مصاب حديثاً. إن «فيروس الإنترنت» المشار إليه على نحو واسع عام 1988م لم يكن فيروساً على الإطلاق، وإنما كان في الواقع دودة.

أسئلة متكررة الطرح حول فيروسات الحاسوب

إن القائمة التالية للأسئلة متكررة الطرح موجودة على المواقع:

- http://www.faqs.org
- Computer virus FAQ for New users:
  http://www.faqs.org/computer-virus/new-users/
- Virus-L/comp.virus FAQ v2.00
  http://www.faqs.org/faqs/computer-virus/faq
- Viruses and the Mac FAQ
  http://www.faqs.org/faqs/computer-virus/macintosh-faq/alt.compp.virusMini-Faq
- http://www.faqs.org/fags/computer-virus/mini-faq/alt.cop.virusFAQpart1/4
- http://www.faqs.org/fags/computer-virus/alt-faq/part1/alt.comp.virusFAQpart2/4
- http://www.faqs.org/fags/computer-virus/alt-faq/part2/alt.comp.virusFAQpart3/4
- http://www.faqs.org/fags/computer-virus/alt-faq/part3/alt.comp.virusFAQpart4/4
- http://www.faqs.org/faqs/computer-virus/alt-faq/part4/

قواعد البيانات التي تعالج ظاهرتي(*): نشر رسالة، والإنذار الكاذب

تلقّى مركز التنسيق CERT في الولايات المتحدة العديد من الاتصالات والرسائل الالكترونية من أشخاص يسألون عمّا إذا كانت الرسالة التي تصلهم عبر البريد الالكتروني صحيحة أم لا؟ قد تساعدك قائمة المصادر الآتية في التميز بين الرسائل أو التحذيرات الكاذبة والصحيحة:

● التحذيرات الكاذبة لشارليز هيمس	Charles Hymes hoaxes http://www.nonprofit.net/hoax
● المقدرة الاستشارية بشأن حوادث الحاسوب	CIAC (computer incident advisory capability)
● الرسائل المخادعة في الإنترنت ـ كيفية تمييز الرسالة المخادعة أو التحذير الصحيح، وما هي الأمور الواجب فعلها؟	Internet hoaxes- how to identify a new hoax or valid warning and what to do? http://hoaxbusters.ciacorg/HBHoaxInfo.html
● التحذيرات المفرطة! ـ مضاد للفيروس	IBM antivirus online- hype alerts! http://www.av.ibm.com/BreakingNews/Hypealert/
● معلومات حول الرسالة المخادعة	ICSA- Hoax Information http://www.icsa.net/html/communuties/antivirus/hoaxes/
● الرسائل المسلسة في الإنترنت ـ كيفية تمييز الرسالة الجديدة المسلسة، ما هي الأمور الواجب فعلها؟	Internet chain letters- how to recognize a new chain letter, what to do? http://www.hoaxbusters.ciac.org/HBHoaxInfo.html
● فيروس الرسالة المخادعة ـ مكتبة المعلومات حول الفيروس ـ McAfee	McAfee- virus Information library- virus hoaxes http://www.vil.mcafee.com/hoax.asp
● الرسائل المخادعة ـ مكتبة الفيروس ـ	Network Associates- virus library- hoaxes http://www.nai.com/asp_set/anti_virus/library/hoaxes.asp

(*) ظاهرتان من ظواهر البريد الإلكتروني، الأولى هي تلقّي رسالة والحضّ على إعادة إرسالها إلى الآخرين chain letter أو نشر رسالة، والثانية هي تلقي إنذار أو تحذير كاذب Hoax.

منشورات ومنظمات حول الفيروس

- (المؤسسة الأوروبية من أجل البحث المضاد للفيروس المتعلق بالحاسوب) EICAR

EICAR (European Institute for Computer Anti-Virus Research)

http://www.eicar.com/

تضم (EICAR) الجامعات، والصناعة ووسائل الإعلام، بالإضافة إلى خبراء القانون والحماية التقنية من الحكومة (مدنياً وقضائياً وعسكرياً) إلى جانب منظمات حماية الخصوصية التي تهدف إلى توحيد الجهود غير الربحية ضد كتابة وتكاثر الرموز الخبيثة مثل أحصنة طروادة أو فيروسات الحاسوب وضد جرائم الحاسوب، والتلاعب وسوء استخدام الحواسيب أو الشبكات، بما في ذلك الاستغلال الماكر لبيانات الموظفين مرتكزة على قانون.

- (الاتحاد العالمي لحماية الحاسوب) ICSA

ICSA (International Computer Security Association)

http://www.icsa.net http://www.icsa.net/html/communities/antivirus http://www.virusbtn.com

يهتم الاتحاد بالمنشورات العالمية حول تجنب، وتمييز وإزالة فيروس الحاسوب. إن نشرة الحاسوب (*Virus Bulletin*) هي مجلة تقنية حول التطورات في مجال فيروسات الحاسوب والمنتجات المضادة للفيروس.

- منظمة اللائحة الحرة الدولية

The Wildlist Organization International

http://www.wildlist.org

إن مهمة منظمة اللائحة الحرة (Wildlist Organization) هي تزويد معلومات شاملة ودقيقة ومناسبة حول فيروسات الحاسوب «in the wild» إلى كل من المستخدمين ومطوري المنتجات.

إن اللائحة الحرة هي قائمة لفيروسات الحاسوب التي وجدت طليقة بدون سيطرة والتي أبلغ عنها بوساطة مجموعة متنوعة مؤلفة من أكثر من 40 متطوعاً مؤهلاً. لقد وضعت هذه القائمة في متناول الجميع مجاناً من قبل المنظمة.

المعايير والمواصفات الحكومية

● (NIST (www.NIST.gov . المواصفات الشائعة من أجل تقييم أمن تقنية المعلومات، 15408، المعيار الشائع /http://csrc.ncsl.nist.gov/cc/ccv20) cc2list.html)

● (NIST. 1995) . في (B.Guttman & E.Roback) مقدمة إلى حماية الحاسوب: دليل(specpub 800-12) the NIST .

● كتاب (DoD orange). معيار (DOD) لتقدير نظام الحاسوب الموثوق، دائرة الدفاع للولايات المتحدة (DoD 5200.28-STD)، نشر في كانون الأول/ ديسمبر عام 1985م.

● منظمة من أجل التطوير والتعاون الاقتصادي (OECD,1992). توجيهات من أجل حماية أنظمة المعلومات، باريس، (OECD,OECD/GD(92)190).

● كتاب (RED 1987). المركز الوطني لحماية الحاسوب. الأداء الموثوق للشبكة، نسخة1,0، NCSC,NCSC-TG-005 .

مراكز الاستجابة للحوادث

● CERT (sm) coordination center

http://www.cert.org/

البريد الالكتروني: cert@cert.org

الهاتف: 412/268-7090

● Computer Incident Advisory Capability (CIAC)

http://ciac.llni.gov/

البريد الالكتروني: ciac@llnl.gov

الهاتف: 925/422-8193

● وكالة أنظمة المعلومات الدفاعية من أجل الأنظمة الآلية:

Defense Information Systems Agency for Automated Systems

فريق دعم حوادث الحماية (المساعدة، لمواقع وزارة الدفاع)

(Security Incident Support Team Cassist, for DOD Sites)

http://www.assist.mil/

البريد الالكتروني : cert@cert.mil

الهاتف : 800/357-4231

- Department of Homeland Security

http://www.uscert.gov

البريد الالكتروني : uscert@uscert.gov

- Federal Computer Incident Response Capability(FEDCIRC)

http://www.fedcirc.gov/

البريد الالكتروني : fedcirc@fedcirc.gov

الهاتف : 888/282-0870

- منتدى فرق الحماية والاستجابة للحوادث:

Forum of Incident Response and Security Teams (FIRST)

http://www.first.org

البريد الالكتروني : first-sec@first.org

- مركز الاستجابة للحادث التابع لـ NASA

NASA Incident Response Center(NASIRC)

http://www-nasirc.nasa.gov/nasa/index.htm

البريد الالكتروني : nasirc@nasirc.nasa.gov

الهاتف : 800/762-7472

- مكتب التحقيقات الفديرالي ـ المركز الوطني لحماية البنية التحتية

(Federal Bureau of Investigation FBI- National Infrastructure Protection Center(NIPC)

http://www.fbi.gov/nipe/index.htm

البريد الالكتروني : nipc@fbi.gov

الاتحادات والمنظمات المتخصصة بأمن المعلومات

- ISSA:(www.issa.org)
- مؤسسة SANS : (www.sans.org)
- الاتحاد العالمي لحماية الحاسوب (International Computer Security Association) ICSA: (www.icsa.net)
- مؤسسة حماية الحاسوب (Computer Security Institute) CSI: (www.gocsi.org)

مواقع إلكترونية مفيدة في أمن المعلومات

http://www.infosyssec.org/infosysec/index.htm

http://www.certicom.com

http://www.counterpane.com

http://www.cs.purdue.edu/coast

http://www.cs.georgetown.edu/˜denning/crypto/index.html

http://www.ntbugtraq.com

http://www.nsi.org/cornpsec.html

http://www.sans.org

http://www.securityportal.com

http://www.icsa.net

http://www.itpolicy.gsa.gov

http://www.cit.nih.gov/security.html

http://cs-www.nist.gov

http://www.bs.org

http://www.rsa.com

http://www.telstra.com.au/info/security.html

المختصرات

المختصر	أصل المختصر	المعنى العربي
AES	Advanced Encryption Standard	معيار التعمية (التشفير) المتقدم
AP	Access Point	نقطة نفاذ
BSS	Basic Service Set	مجموعة الخدمة الأساسية
CART	Computer Analysis Response Team	فريق الاستجابة للتحليل الحاسوبي
CERTs	Computer Emergency Response Teams	فرق الاستجابة لطوارئ الحاسوب
CFO	Chief Finance Officer	المدير المالي
CISO	Chief Information Security Officer	مسؤول أمن المعلومات الرئيسي
COOP	Contingency Operation Plan	خطة عمليات الطوارئ
COTS	Commercial Of The Shelf	متوفرة تجارياً في السوق
CRM	Customer Relation Management	إدارة العلاقة مع الزبون
DHCP	Dynamic Host Configuration Protocol	بروتوكول بناء (توضيب) الحاسوب المضيف ديناميكياً
DHS	Department of Homeland Security	وزارة الأمن الوطني(الأمريكية)
DOD	Department Of Defense	وزارة الدفاع (الأمريكية)
DOS	Denial Of Service	حرمان من الخدمة
EAP	Extensible Authentication Protocol	بروتوكول التحقق من الهوية الموسع
EDI	Electronic Data Interchange	تبادل البيانات الإلكتروني
ERP	Enterprise Resource Planning	التخطيط لموارد المؤسسة
ESS	Extended Service Set	مجموعة الخدمة الموسعة
EUA	Enterprise-level User Authentication	معيار التحقق من هوية المستخدم بمستوى المؤسسة
FBI	Federal Bureau of Investigation	مكتب التحقيقات الفيدرالي
FEAF	Federal Enterprise Architecture Framework	الإطار المعماري للمؤسسة الفيدرالية

GPS	Global Positioning System	النظام العالمي لتحديد الموقع
HIPAA	Health Insurance Portability and Accountability Act.	قانون المساءلة الخاص بالضمان الصحي (الأمريكي)
IA	Information Assurance	تأمين المعلومات
IBSS	Independent Basic Service Set	مجموعة الخدمة الأساسية المستقلة
IDS	Intrusion Detection System	نظام كشف الاختراق
IFCC	Internet Fraud Compliance Center	مركز الادعاء ضد التلاعب عبر الإنترنت
INFOSEC	Information Security	(نموذج زاشمان) لأمن المعلومات
IP	Internet Protocol	بروتوكول الإنترنت
IRS	Internal Revenue Service	خدمة الإيراد الداخلي
IV	Initialization Vector	متجه الابتداء
LAN	Local Area Network	شبكة حاسوب محلية
MAC address	Media Access Control Address	عنوان التحكم بالنفاذ إلى الوسائط (هوية الجهاز مجسدة فيه)
MIC	Message Integrity Check	فحص سلامة الرسالة
NIC	Network Interface Card	بطاقة الربط مع الشبكة
PDA	Personal Digital Assistant	مساعد شخصي رقمي
PKI	Public Key Infrastructure	البنية التحتية للمفتاح العام
SLAs	Service Level Agreements	اتفاقيات مستوى الخدمة
SMS	Software Management Servers	مخدمات إدارة البرمجيات
SOHO	Small Office/Home Office	مكتب العمل أو المنزل
SOPs	Standard Operational Procedures	إجراءات العمل المعيارية (القياسية)
SSID	Service Set Identifier	مُعَرِّف مجموعة الخدمة
TKIP	Temporal Key Integrity Protocol	بروتوكول سلامة المفتاح المؤقت
VPN	Virtual Private Network	شبكة خاصة افتراضية
WAP	Wireless Access Point	نقطة نفاذ لاسلكي
WEP	Wired Equivalent Privacy	خصوصية مكافئة للشبكات السلكية
WEP	Wireless Encryption Protocol	بروتوكول التعمية اللاسلكي
WLAN	Wireless Local Area Network	شبكة حاسوب محلية لاسلكية
WPA	Wi-Fi Protected Access	النفاذ المحمي لشبكة Wi-Fi

ثبت المصطلحات
(عربي ــ إنجليزي)

اختطاف	Hijacking
الأخلاقية	Ethicality
أسهم	Shares of stock
أصحاب المصلحة	Stake holders
أعمال الغش والخداع	Fraud schemes
أمن	Security
إنذار كاذب	Hoax
باب مفخخ	Trap door
برمجيات خبيثة	malware
برمجيات مجسدة (مخزونة)	Firmware
بفاعلية	Effectively
البقعة الساخنة	Hot spot
بكفاءة، بمردودية	Efficiently
البنية (تحديد وضع)	Configuration
تحديث	Upgrade
تحسين	Enhancement
التحقق من الهوية	Authentication
التحكم بالنفاذ	Access control
تحيين	Up-date
تخزين احتياطي	Back-up
ترقيعات	Patches

Validate	تفحّص
Internet protocol scanner	تفقد بروتوكول الإنترنت
Authorization	التفويض
Risk assessment	تقييم أثر المخاطر
Assessment	تقييم الأثر
Packet sniffer	تلصص على كتل المعلومات
Software installation	تنصيب البرمجيات
Notarization	التوثيق
Vulnerabilities	ثغرات
Trust	الثقة
Availability	الجاهزية
Wireless wall	الجدار اللاسلكي
Zombie	حاسوب مسلوب الإرادة (مسكون)
War driving	التحرّي بالسيارة
War dialing	التحرّي بالهاتف
Chain letter	الحض على إعادة إرسال رسالة (بريد إلكتروني)
Protection	حماية
Spoofing	خداع
Privacy	الخصوصية
LAN jacking	خطف الشبكات
Information defense in depth	الدفاع المعمق عن المعلومات
Life Cycle	دورة حياة
Confidentiality	السِّرية
Integrity	السلامة
Supply chain	سلسلة التزويد
Business process	سيرورة الأعمال
Controls	ضوابط
Noninterference	عدم التدخل (عدم التشويش)

Non-repudiation	عدم إنكار التواصل
Accountability	قابلية المساءلة
Hacker	قرصان (على شبكة الإنترنت)
Sniffer	متلصلص
Cracker	مخترق (على شبكة الإنترنت)
log	مدونة (سجل) الحوادث
Share holders	المساهمين
Data warehouse	مستودع بيانات
Security clearance	موافقة أمنية
Router	مُوَجِّه
Redundancy systems	نظم احتياطية
Hub	نقطة تَجَمُّع

ثبت المصطلحات
(إنجليزي ــ عربي)

Access control	التحكم بالنفاذ
Accountability	قابلية المساءلة
Assessment	تقييم الأثر
Authentication	التحقق من الهوية
Authorization	التفويض
Availability	الجاهزية
Back-up	تخزين احتياطي
Business process	سيرورة الأعمال
Chain letter	الحض على إعادة إرسال رسالة (بريد إلكتروني)
Confidentiality	السِّرية
Configuration	البنية (تحديد وضع)
Controls	ضوابط
Cracker	مخترق (على شبكة الإنترنت)
Data warehouse	مستودع بيانات
Effectively	بفاعلية
Efficiently	بكفاءة، بمردودية
Enhancement	تحسين
Ethicality	الأخلاقية
Firmware	برمجيات مجسدة (مخزونة)
Fraud schemes	أعمال الغش والخداع
Hacker	قرصان(على شبكة الإنترنت)

Hijacking	اختطاف
Hoax	إنذار كاذب
Hot spot	البقعة الساخنة
Hub	نقطة تَجَمُّع
Information defense in depth	الدفاع المعمق عن المعلومات
Integrity	السلامة
Internet protocol scanner	تفقد بروتوكول الإنترنت
LAN jacking	خطف الشبكات
Life Cycle	دورة حياة
log	مدونة (سجل) الحوادث
malware	برمجيات خبيثة
Noninterference	عدم التدخل (عدم التشويش)
Non-repudiation	عدم إنكار التواصل
Notarization	التوثيق
Packet sniffer	تلصص على كتل المعلومات
Patches	ترقيعات
Privacy	الخصوصية
Protection	حماية
Redundancy systems	نظم احتياطية
Risk assessment	تقييم أثر المخاطر
Router	موجه
Security	أمن
Security clearance	موافقة أمنية
Share holders	المساهمين
Shares of stock	أسهم
Sniffer	متلصص
Software installation	تنصيب البرمجيات
Spoofing	خداع

Stake holders	أصحاب المصلحة
Supply chain	سلسلة التزويد
Trap door	باب مفخخ
Trust	الثقة
Up-date	تحيين
Upgrade	تحديث
Validate	تفحّص
Vulnerabilities	ثغرات
War dialing	التحري بالمودم
War driving	التحري بالسيارة
Wireless wall	الجدار اللاسلكي
Zombie	حاسوب مسلوب الإرادة (مسكون)

المراجـع

Alliance, W. F. (2003). *Wi-Fi Protected Access: An Overview*. Retrieved 5 February 2004, from http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf.

Austin, R. (2001). *The iPremier Company (a): Denial of Service Attack*. Harvard Business School, 9-601-114 (rev. 13 June 2002). Boston, MA: Harvard Business School Publishing.

Beach, G. (2003, April 1). Certify security. *CIO Magazine*: 12, 16.

Cranite. (2003). *Wireless Wall® Technical Operation White Paper. Retrieved 7 February 2004, from http://www.cranite.com/pdf/whitepapers/wirelesswall-tech-op.pdf.*

Curtin, M., and. Ranum, M. J. *Internet Firewalls: Frequently Asked Questions*. Date: 2000/12/01 19:48:21. Revision: 10.0. Downloaded 14 February 2004 from http://www.faqs.org/faqs/firewalls-faq.

Farnan, J. E. (2003). *Fighting Fraud: Improving Information Security*. Federal Bureau of Investigation, Washington, D.C., 3 April, Downloaded on 15 February 2004 from http://www.fbi.gov/congress/congress03/farnan040303.htm.

Fluhrer, S., Mantin, I., and Shamir, A. (2001). «Weaknesses in the Key Scheduling Algorithm or RC4.» *Eighth Annual Workshop on Selected Areas in Cryptography*.

FTC (2004). *Report on Consumer Complaints*.

Gehrke, R. (2003). «Quick Consumer Notification Key in Identity Theft Cases,» *USA Today:* 6 November, Retrieved 15 February 2004 from http://www.usatoday.com/tech.news/internetprivacy/2003-11- 06-id-theft-tips_x.htm

Gordon, B. (2003). *21 Tips for Improved Wireless Security*. Unpublished.

IEEE (2001). *802.11b-1999 Wireless LANs (802.11)*. Retrieved 4 February 2004, from http://standards.ieee.org/reading/ieee/std/lanman/restricted/802.11b-1999.pdf.

Karygiannis, T., and Owmes, L. (2002). *Wireless Network Security: 802.11, Bluetooth™ and Handheld Devices*. Retrieved 4 February 2004, from http://csrc.nist.gov/publications/drafts/draft-sp800- 48.pdf.

Kim, G., and Shin, J. G. (2003). *Proposal for a Secure Wireless LAN System in Which the RF Signal is Invisible to Unauthorized Observers and Intruders*.

Lewicki, R. J. and Bunker, B. B. (1996). «Developing and Maintaining Trust in Work Relationships.» In: R. M. Kramer and T.R. Tyler (eds.). *Trust in Organizations - Frontiers of Theory and Research*. London: Sage Publications.

Maconachy, W. [et al.] (2001). «A Model for Information Assurance: An integrated Approach.» Paper presented at: *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 5-6 June. Figures 1 and 2 are also taken from this paper.

Musgrove, M. (2004). «Tech Experts Downplay Theft of Windows Code.» *Washington Post:* 14 February, E1.

Nolan, R. (2001). «Q&A with Harvard Business School's Dr. Richard Nolan: IT Business Strategies in the Network Era.» *Harvard Business Review:* 29 June.

Reid, N., and Seide, R. (2003). *802.11 (Wi-Fi) Networking Handbook*. New York: McGraw-Hill. p. 182.

Reiner, R. (dir.) (1984). *This Is Spinal Tap* [Motion picture]. United States: Metro Goldwyn Mayer.

Al-Saleh, A. (2002). *Secure, Seamless Roaming Leads to an Ideal Wireless Experience*. Retrieved 3 February 2004, from http://www.tmcnet.com/bizwatch/articales/090402a.htm.

SetSolutions, Inc. (2004). Retrieved 4 February 2004 from http://www. setsolutions.com/security.html.

Stubblefield, A., Ioannidis, J. and Rubin, A. D. (2001). *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP* (No. TD-4ZCPZZ). AT&T Labs.

حول مؤلفي الكتاب

لورنس أم. أوليفا: هو مدير «إدارة مشروع البنية التحتية» لمشروع التحالف (CSCPRIME) الذي يركز على تجديد العديد من الاتصالات والبنية التحتية المتعلقة بالحاسوب التابعة لوزارة المالية في الولايات المتحدة. لديه خبرة أكثر من 25 سنة بإجراءات وممارسات أمن المعلومات من وجهتي نظر الإدارة التنفيذية والتقنية، ولقد نفذ العديد من الممارسات الأفضل لإدارة أمن المعلومات المذكورة في هذا الكتاب. بوصفه محترفاً مجازاً في إدارة المشاريع (PMP)، أدار أوليفا عدة مشاريع استثنائية هامة وبالغة الخطورة، قد وصلت إلى 160 مليون دولار في الميزانية. وباعتباره نائباً لرئيس شركة تختص بأمن الحاسوب تطور حلول الحماية البيولوجية، فإن فريقه قد قام بتطوير وتركيب الإجراءات اللازمة للانتقال بسرعة وأمن ورخص لمئات مستخدمي تقنية المعلومات للرعاية الصحية والمالية من أوضاع كلمة السِّر فقط إلى بيئات الدخول البيولوجي للحماية العالية متعددة الطرق. وهو عضو في هيئة التدريس لجامعة فونيكس.

تعمل **كريسان هيرود** في جامعة الدفاع الوطني كرئيسة قسم عمليات المعلومات وقسم تأمين المعلومات، حيث إنها مسؤولة عن المناهج بما في ذلك العمليات وتأمين وأمن المعلومات، بالإضافة إلى كونها أستاذة جامعية لمادتي إدارة الأنظمة وأمن المعلومات. لقد كانت سابقاً مديرة أمن تقنية المعلومات الشاملة في غلاكسو سميث كلاين (gsk) وهي الشركة الضخمة للمستحضرات الصيدلية، كما كانت مديرة لأمن المعلومات في «فاني مي» وهو الاتحاد الفيدرالي لقروض السكن. عندما كانت في «فاني مي» عملت في شراكة مدعومة من البيت الأبيض من أجل الحماية الحرجة للبينة التحتية كرئيسة لمجموعة عمل في تحليل ومشاركة المعلومات، وهي الآن مستشارة خاصة لتحرك مركز تحليل ومشاركة المعلومات لصناعة العناية الصحية. إنها مساعدة

أستاذ جامعي تقوم بتدريس مواد القيادة وأمن المعلومات في جامعتي فيرفاكس و فونيكس. لقد دَرَّست من عام 1999 إلى عام 2001م مواد أمن المعلومات لطلاب الدراسات العليا في جامعة جورج واشنطن.

إن **كريج أي. كوشر** هو أستاذ جامعي لتأمين المعلومات وعملياتها في جامعة الدفاع الوطني. عمل في مجموعة متنوعة من المناصب لإدارة الأنظمة وأمن المعلومات، من المستوى التكتيكي إلى المستوى الاستراتيجي، وفي مجتمع الاستخبارات الأمريكية لأكثر من 21 عاماً في مهنة الخدمة العسكرية. حصل على بكالوريوس في الاتصالات من جمعة تيمبل وماجستير في إدارة هندسة البرمجيات من جامعة ميشيغان المركزية وهو حالياً يحضّر الدكتوراة في نظم المعلومات. حائز كذلك على شهادتي التخرج CISO و CIO من وزارة الدفاع وهو مدير مجاز في أمن المعلومات (CISM). لقد قام بنشر مقالات حول محاور متعددة في أمن المعلومات وتحدث في مؤتمرات صناعية وحكومية عديدة.

ل.ت.سي. كليفتون هـ. بوول IAM، CISM، CISSP هو جندي محنك مع خبرة في الجيش الأمريكي لمدة 20 عاماً. يُدَرِّس كليفتون هـ. بوول حالياً تأمين المعلومات، ورسم السياسة، ومعايير الحماية والأمن اللاسلكية في كلية إدارة مصادر المعلومات في جامعة الدفاع الوطني ـ واشنطن DC. لقد تميز في جريدة بوست واشنطن عام 2003م لبحثه في الأمور الحاسوبية اللاسلكية باعتباره رسم خريطة لنقاط الوصول اللاسلكية المحلية. إنه طالب دكتوراه في علوم المعلومات والحاسوب، جامعة جنوب شرغي نوفا.

تشاليز ريكس الرابع (IV) هو كبير موظفي المعلومات ومدير العمليات الأكاديمية في كلية الحرب. الوطنية في واشنطن DC حصل على شهادة البكالوريوس من معهد فيرجينيا الحربي وماجستير في إدارة الأعمال من جامعة فونيكس، كما أنه حائز على شهادة كبير موظفي المعلومات وشهادة تأمين المعلومات من كلية إدارة مصادر المعلومات في جامعة الدفاع الوطني. يقتني السيد ريكس مؤسسة استشارات، وهو عضو في هيئة التدريس والإدارة في جامعة فونيكس.

فهـــــرس

ـ أ ـ

- ب -

ـ ت ـ

- د -

- ر -

- ز -

- س -

- ش -

- ك -

- ل -

- م -

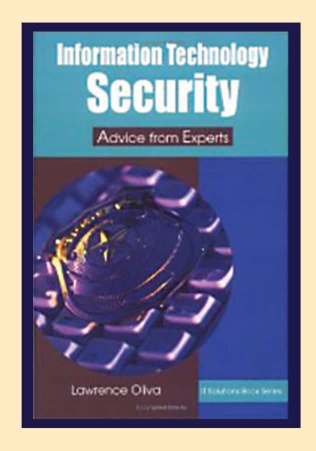
- ن -

- هـ -

- و -

- ي -

أمن تقنية المعلومات(*)
نصائح من خبراء



(*) الكتاب الثالث من تقنية المعلومات

السلسلة: تضم هذه السلسلة ترجمة لأحدث الكتب عن التقنيات التي يحتاج إليها الوطن العربي في البحث والتطوير ونقل المعرفة إلى القارئ العربي.

الكتاب: مع تزايد قيمة المعلوماتية تطورت الأمنيّة المعلوماتية من مجرد منظور إنتاجي إلى سيرورة إدارة أعمال.

ولم تعد أمنيّة المعلومات اليوم عملية تحكّم في مدخلات البيانات والأنظمة، وإنما السيطرة على مجموعة الخدمات، ومن ضمنها الشبكات اللاسلكية، والحماية من قرصنة المعلومات، بالإضافة إلى مداومة التخطيط العملياتي في حالات الكوارث.

على أساس هذه المفاهيم تغيّرت استراتيجية تنفيذ تكنولوجيا المعلومات من مجرّد مواجهة التحديات الخارجية إلى تكوين بنية تحتية للحماية موثوق بها ومرتبطة بسيرورات العمل، وذلك لتحريك العائدات المالية، وجني الأرباح.

تمثّل سلسلة IT للحلول، ومنها كتابنا: **أمن تقنية المعلومات: نصائح من خبراء**، حصيلة لقاءات ومقابلات مع اختصاصيين وممارسين في حقل المعلوماتية، منحونا وجهات نظرهم حول نجاحات وفشل حماية المعلوماتية في المنظمات.

المؤلف: **لورنس م. أوليفا:** متخصّص في نظم المعلومات، والصناعات الإلكترونية، وله خبرة في مجال نظم معلوماتية الفضاء والطيران، زادت على عشرين عاماً. يعمل أوليفا حالياً مع شركة NCR ويستخدم معظم ما جاء في هذا الكتاب من تقنيات في التخاطب مع أعضاء فريقه على بعد أمتار، أو كيلومترات منه.

المترجم: **محمد مراياتي:** دكتوراه دولة في الفيزياء، عمل مديراً لمعهد بحوث الإلكترونيات والعلوم الأساسية في دمشق، ثم مديراً للمعهد العالي للعلوم التطبيقية والتكنولوجيا فيها، ثم مستشاراً في الأمم المتحدة (الإسكوا)، ثم كبير مستشاري العلوم والتكنولوجيا للتنمية المستدامة UN-DESA. ويعمل حالياً مستشاراً في وزارة الاقتصاد والتخطيط في المملكة العربية السعودية.

سلسلة كتب التقنيات الاستراتيجية والمتقدّمة

1. **المياه**
2. **البترول والغاز**
3. **البتروكيمياء**
4. **النانو**
5. **التقنية الحيوية**
6. **تقنية المعلومات**
7. **الإلكترونيات والاتصالات والضوئيات**
8. **الفضاء والطيران**
9. **الطاقة**
10. **المواد المتقدمة**
11. **البيئة**



المنظمة العربية للترجمة

مدينة الملك عبدالعزيز للعلوم والتقنية KACST

أمن تقنية المعلومات — نصائح من خبراء — لورنس م. أوليفا

(6-3)

الثمن: 18 دولاراً أو ما يعادلها

ISBN 978-9953-82-403-1
9 789953 824031